Guide de l’utilisateur

AWS Deadline Cloud

Version latest

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

AWS Deadline Cloud: Guide de l’utilisateur

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

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que AWS Deadline Cloud ?

Deadline Cloud est un Service AWS outil que vous pouvez utiliser pour créer et gérer des projets et des tâches de rendu sur des instances Amazon Elastic Compute Cloud (Amazon EC2) directement à partir de pipelines de création de contenu numérique et de postes de travail.

Deadline Cloud fournit des interfaces de console, des applications locales, des outils de ligne de commande et une API. Avec Deadline Cloud, vous pouvez créer, gérer et surveiller des fermes, des flottes, des tâches, des groupes d'utilisateurs et des espaces de stockage. Vous pouvez également définir les exigences matérielles, créer des environnements pour des charges de travail spécifiques et intégrer les outils de création de contenu nécessaires à votre production dans votre pipeline Deadline Cloud.

Deadline Cloud fournit une interface unifiée pour gérer tous vos projets de rendu en un seul endroit. Vous pouvez gérer les utilisateurs, leur attribuer des projets et accorder des autorisations pour les rôles professionnels.

Rubriques

Caractéristiques de Deadline Cloud

Voici quelques-unes des principales manières dont Deadline Cloud peut vous aider à exécuter et à gérer les charges de travail de calcul visuel :

- Créez rapidement vos fermes, vos files d'attente et vos flottes. Surveillez leur statut et obtenez un aperçu du fonctionnement de votre ferme et de vos emplois.
- Gérez de manière centralisée les utilisateurs et les groupes de Deadline Cloud et attribuez des autorisations.

- Gérez la sécurité de connexion pour les utilisateurs du projet et les fournisseurs d'identité externes avec AWS IAM Identity Center.
- Gérez en toute sécurité l'accès aux ressources du projet à l'aide de politiques et de rôles AWS Identity and Access Management (IAM).
- Utilisez des balises pour organiser et retrouver rapidement les ressources du projet.
- Gérez l'utilisation des ressources du projet et les coûts estimés de votre projet.
- Proposez un large éventail d'options de gestion du calcul pour prendre en charge le rendu dans le cloud ou en personne.

Concepts et terminologie pour Deadline Cloud

Pour vous aider à démarrer avec AWS Deadline Cloud, cette rubrique explique certains de ses principaux concepts et termes.

Directeur du budget

: Le gestionnaire de budget fait partie du moniteur Deadline Cloud. Utilisez le gestionnaire de budget pour créer et gérer des budgets. Vous pouvez également l'utiliser pour limiter les activités afin de respecter le budget.

Bibliothèque cliente Deadline Cloud

: La bibliothèque client inclut une interface de ligne de commande et une bibliothèque pour gérer Deadline Cloud. Les fonctionnalités incluent la soumission de lots de tâches basés sur la spécification Open Job Description à Deadline Cloud, le téléchargement des résultats des pièces jointes aux tâches et la surveillance de votre ferme à l'aide de l'interface de ligne de commande.

Application de création de contenu numérique (DCC)

: Les applications de création de contenu numérique (DCC) sont des produits tiers dans lesquels vous créez du contenu numérique. Des exemples de DCC sont MayaNuke, et. Houdini Deadline Cloud fournit des plugins intégrés aux soumetteurs de tâches pour des DCC spécifiques.

Farm

: Une ferme est l'endroit où se trouvent les ressources de votre projet. Il se compose de files d'attente et de flottes.

Flotte

Une flotte est un groupe de nœuds de travail qui effectuent le rendu. Les nœuds de travail traitent les tâches. Une flotte peut être associée à plusieurs files d'attente, et une file d'attente peut être associée à plusieurs flottes.

Tâche

Une tâche est une demande de rendu. Les utilisateurs soumettent des offres d'emploi. Les tâches contiennent des propriétés de tâche spécifiques décrites sous forme d'étapes et de tâches.

Pièces jointes aux offres d'emploi

Une pièce jointe à une tâche est une fonctionnalité de Deadline Cloud que vous pouvez utiliser pour gérer les entrées et les sorties des tâches. Les fichiers de tâches sont téléchargés sous forme de pièces jointes au cours du processus de rendu. Ces fichiers peuvent être des textures, des modèles 3D, des appareils d'éclairage et d'autres éléments similaires.

Propriétés de la tâche

Les propriétés de la tâche sont des paramètres que vous définissez lorsque vous soumettez une tâche de rendu. Parmi les exemples, citons la plage d'images, le chemin de sortie, les pièces jointes aux tâches, la caméra rendable, etc. Les propriétés varient en fonction du DCC à partir duquel le rendu est soumis.

Modèle de tâche

Un modèle de tâche définit l'environnement d'exécution et tous les processus exécutés dans le cadre d'une tâche Deadline Cloud.

File d’attente

Une file d'attente est l'endroit où se trouvent les tâches soumises et où leur rendu est prévu. Une file d'attente doit être associée à une flotte pour que le rendu soit réussi. Une file d'attente peut être associée à plusieurs flottes.

Association des flottes de files d'attente

Lorsqu'une file d'attente est associée à une flotte, il existe une association entre file d'attente et flotte. Utilisez une association pour planifier les travailleurs d'un parc pour les tâches de cette file d'attente. Vous pouvez démarrer et arrêter des associations pour contrôler la planification du travail.

Étape

Une étape est un processus spécifique à exécuter dans le cadre de la tâche.

Expéditeur de Deadline Cloud

Un émetteur de Deadline Cloud est un plugin de création de contenu numérique (DCC). Les artistes l'utilisent pour soumettre des offres d'emploi à partir d'une interface DCC tierce qu'ils connaissent bien.

Balises

Une étiquette est une étiquette que vous pouvez attribuer à une AWS ressource. Chaque balise est composée d'une clé et d'une valeur facultative que vous définissez.

Grâce aux balises, vous pouvez classer vos AWS ressources de différentes manières. Par exemple, vous pouvez définir un ensemble de balises pour les instances Amazon EC2 de votre compte afin de suivre le propriétaire et le niveau de pile de chaque instance.

Vous pouvez également classer vos AWS ressources par objectif, propriétaire ou environnement. Cette approche est utile lorsque vous disposez de nombreuses ressources du même type. Vous pouvez identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées.

Tâche

Une tâche est un composant unique d'une étape de rendu.

Licences basées sur l'utilisation (UBL)

Les licences basées sur l'utilisation (UBL) sont un modèle de licence à la demande disponible pour certains produits tiers. Ce modèle est payant au fur et à mesure, et vous êtes facturé en fonction du nombre d'heures et de minutes que vous utilisez.

Explorateur d'utilisation

L'explorateur d'utilisation est une fonctionnalité du moniteur Deadline Cloud. Il fournit une estimation approximative de vos coûts et de votre utilisation.

Nœuds

Les travailleurs appartiennent à des flottes et exécutent les tâches assignées par Deadline Cloud pour effectuer les étapes et les tâches. Les employés stockent les journaux des opérations liées aux tâches dans Amazon CloudWatch Logs. Les employés peuvent également utiliser la fonctionnalité de pièces jointes aux tâches pour synchroniser les entrées et les sorties avec un bucket Amazon Simple Storage Service (Amazon S3).

Commencer à utiliser Deadline Cloud

Utilisez Deadline Cloud pour créer rapidement un parc de rendu avec des paramètres et des ressources par défaut, tels que la configuration de l'instance Amazon EC2 et les compartiments Amazon Simple Storage Service (Amazon S3).

Vous pouvez également définir les paramètres et les ressources lorsque vous créez un parc de rendu. Cette méthode prend plus de temps que l'utilisation des paramètres et des ressources par défaut, mais elle vous donne plus de contrôle.

Une fois que vous serez familiarisé avec les concepts et la terminologie de Deadline Cloud, consultez la section Mise en route pour obtenir des step-by-step instructions sur la création de votre ferme, l'ajout d'utilisateurs et des liens vers des informations utiles.

Accès à Deadline Cloud

Vous pouvez accéder à Deadline Cloud de l'une des manières suivantes :

- Console Deadline Cloud : accédez à la console dans un navigateur pour créer une ferme et ses ressources, et gérer l'accès des utilisateurs. Pour plus d'informations, consultez la section Mise en route.
- Deadline Cloud monitor : gérez vos tâches de rendu, notamment en mettant à jour les priorités et les statuts des tâches. Surveillez votre ferme et consultez les journaux et le statut des tâches. Pour les utilisateurs disposant d'autorisations de propriétaire, le moniteur Deadline Cloud permet également d'explorer l'utilisation et de créer des budgets. Le moniteur Deadline Cloud est disponible à la fois sous forme de navigateur Web et d'application de bureau.
- AWS SDK et AWS CLI — Utilisez le AWS Command Line Interface (AWS CLI) pour appeler les opérations de l'API Deadline Cloud depuis la ligne de commande de votre système local. Pour plus d'informations, consultez la section Configuration d'un poste de développement.

Services connexes

Deadline Cloud fonctionne avec les solutions suivantes Services AWS :

- Amazon CloudWatch — Avec CloudWatch, vous pouvez suivre vos projets et les AWS ressources associées. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

- Amazon EC2 —Cela Service AWS fournit des serveurs virtuels qui exécutent vos applications dans le cloud. Vous pouvez configurer vos projets pour utiliser des instances Amazon EC2 pour vos charges de travail. Pour plus d'informations, consultez Instances Amazon EC2.
- Amazon EC2 Auto Scaling — Avec Auto Scaling, vous pouvez automatiquement augmenter ou diminuer le nombre d'instances en fonction de l'évolution de la demande sur vos instances. Auto Scaling permet de s'assurer que vous exécutez le nombre d'instances souhaité, même en cas de défaillance d'une instance. Si vous activez Auto Scaling avec Deadline Cloud, les instances lancées par Auto Scaling sont automatiquement enregistrées auprès de la charge de travail. De même, les instances mises hors service par Auto Scaling sont automatiquement désenregistrées de la charge de travail. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
- AWS PrivateLink— AWS PrivateLink fournit une connectivité privée entre les clouds privés virtuels (VPC) et vos réseaux sur site, sans exposer votre trafic à l'Internet public. Services AWS AWS PrivateLink permet de connecter facilement les services entre différents comptes et VPC. Pour plus d'informations, consultez AWS PrivateLink.
- Amazon S3 — Amazon S3 est un service de stockage d'objets. Deadline Cloud utilise des compartiments Amazon S3 pour stocker les pièces jointes aux tâches.
- IAM Identity Center — IAM Identity Center est un Service AWS endroit où vous pouvez fournir aux utilisateurs un accès par authentification unique à tous les comptes et applications qui leur sont attribués à partir d'un seul endroit. Vous pouvez également gérer de manière centralisée l'accès à plusieurs comptes et les autorisations des utilisateurs pour tous vos comptes. AWS Organizations Pour de plus amples informations, veuillez consulter Questions fréquentes (FAQ)AWS IAM Identity Center.

Comment fonctionne Deadline Cloud

Avec Deadline Cloud, vous pouvez créer et gérer des projets et des tâches de rendu directement à partir de pipelines et de postes de travail de création de contenu numérique (DCC).

Vous soumettez des tâches à Deadline Cloud à l'aide du AWS SDK, AWS Command Line Interface (AWS CLI) ou des émetteurs de tâches de Deadline Cloud. Deadline Cloud prend en charge l'Open Job Description (OpenJD) pour la spécification des modèles de tâches. Pour plus d'informations, consultez Open Job Description sur le GitHub site Web.

Deadline Cloud fournit des soumissionnaires d'offres d'emploi. Un émetteur de tâches est un plugin DCC permettant de soumettre des tâches de rendu à partir d'une interface DCC tierce, telle que

ou. Maya Nuke Avec un émetteur, les artistes peuvent soumettre des travaux de rendu depuis une interface tierce à Deadline Cloud, où les ressources du projet sont gérées et les tâches sont surveillées, le tout en un seul endroit.

Avec une ferme Deadline Cloud, vous pouvez créer des files d'attente et des flottes, gérer les utilisateurs et gérer l'utilisation des ressources et les coûts du projet. Une ferme se compose de files d'attente et de flottes. Une file d'attente est l'endroit où se trouvent les tâches soumises et où leur rendu est prévu. Une flotte est un groupe de nœuds de travail qui exécutent des tâches pour effectuer des tâches. Une file d'attente doit être associée à un parc afin que les tâches puissent être affichées. Une seule flotte peut prendre en charge plusieurs files d'attente et une file d'attente peut être prise en charge par plusieurs flottes.

Les tâches se composent d'étapes, et chaque étape comprend des tâches spécifiques. Avec le moniteur Deadline Cloud, vous pouvez accéder aux statuts, aux journaux et à d'autres indicateurs de résolution des problèmes relatifs aux tâches, aux étapes et aux tâches.

Autorisations dans Deadline Cloud

Deadline Cloud prend en charge les fonctionnalités suivantes :

- Gérer l'accès à ses opérations d'API à l'aide de AWS Identity and Access Management (IAM)
- Gestion de l'accès des utilisateurs du personnel à l'aide d'une intégration avec AWS IAM Identity Center

Avant que quiconque puisse travailler sur un projet, il doit avoir accès à ce projet et à la ferme associée. Deadline Cloud est intégré à IAM Identity Center pour gérer l'authentification et l'autorisation du personnel. Les utilisateurs peuvent être ajoutés directement à IAM Identity Center, ou celui-ci peut être connecté à votre fournisseur d'identité (IdP) Okta existant comme ou. Active Directory Les administrateurs informatiques peuvent accorder des autorisations d'accès aux utilisateurs et aux groupes à différents niveaux. Chaque niveau suivant inclut les autorisations des niveaux précédents. La liste suivante décrit les quatre niveaux d'accès, du niveau le plus bas au niveau le plus élevé :

- Visionneur : autorisation de voir les ressources des fermes, des files d'attente, des flottes et des emplois auxquels elles ont accès. Un utilisateur ne peut pas soumettre de tâches ou y apporter des modifications.

- Contributeur : identique à un téléspectateur, mais avec l'autorisation de soumettre des tâches à une file d'attente ou à un parc de serveurs.
- Gestionnaire : identique au contributeur, mais il est autorisé à modifier les tâches dans les files d'attente auxquelles il a accès et à accorder des autorisations sur les ressources auxquelles il a accès.
- Propriétaire — Identique au responsable, mais il peut consulter et créer des budgets et voir l'utilisation.

> **Note**
>
> Ces autorisations ne permettent pas aux utilisateurs d'accéder à l'infrastructure de Deadline Cloud AWS Management Console ou de la modifier.

Les utilisateurs doivent avoir accès à une ferme avant de pouvoir accéder aux files d'attente et aux flottes associées. L'accès des utilisateurs est attribué aux files d'attente et aux flottes séparément au sein d'un parc.

Vous pouvez ajouter des utilisateurs en tant qu'individus ou en tant que membres d'un groupe. L'ajout de groupes à une ferme, à une flotte ou à une file d'attente peut faciliter la gestion des autorisations d'accès pour de grands groupes de personnes. Par exemple, si une équipe travaille sur un projet spécifique, vous pouvez ajouter chacun des membres de l'équipe à un groupe. Vous pouvez ensuite accorder des autorisations d'accès à l'ensemble du groupe pour la ferme, le parc ou la file d'attente correspondants.

Support logiciel avec Deadline Cloud

Deadline Cloud fonctionne avec n'importe quelle application logicielle qui peut être exécutée à partir d'une interface de ligne de commande et contrôlée à l'aide de valeurs de paramètres. Deadline Cloud prend en charge la OpenJD spécification permettant de décrire le travail sous forme de tâches comportant des étapes de script logiciel paramétrées (par exemple sur une plage d'images) en tâches. Rassemblez OpenJD les instructions de travail dans des ensembles de tâches avec les outils et fonctionnalités de Deadline Cloud pour créer, exécuter et licencier les étapes à partir d'une application logicielle tierce.

Les travaux nécessitent une licence pour être rendus. Deadline Cloud propose des licences basées sur l'utilisation (UBL) pour une sélection de licences d'applications logicielles facturées à l'heure

par tranches de minutes en fonction de l'utilisation. Avec Deadline Cloud, vous pouvez également utiliser vos propres licences logicielles si vous le souhaitez. Si une tâche ne peut pas accéder à une licence, elle ne s'affiche pas et produit une erreur qui s'affiche dans le journal des tâches du moniteur Deadline Cloud.

Commencer à utiliser Deadline Cloud

Pour créer un parc dans AWS Deadline Cloud, vous pouvez utiliser la console Deadline Cloud ou le AWS Command Line Interface (AWS CLI). Utilisez la console pour une expérience guidée de création de la ferme, y compris des files d'attente et des flottes. Utilisez-le AWS CLI pour travailler directement avec le service ou pour développer vos propres outils compatibles avec Deadline Cloud.

Pour créer une ferme et utiliser le moniteur Deadline Cloud, configurez votre compte pour Deadline Cloud. Vous ne devez configurer l'infrastructure de surveillance de Deadline Cloud qu'une seule fois par compte. Depuis votre ferme, vous pouvez gérer votre projet, y compris l'accès des utilisateurs à votre ferme et à ses ressources.

Pour créer une ferme sans configurer l'infrastructure de surveillance de Deadline Cloud, configurez un poste de travail de développement pour Deadline Cloud.

Pour créer une ferme avec un minimum de ressources pour accepter des tâches, sélectionnez Quickstart sur la page d'accueil de la console. Configurer le moniteur Deadline Cloudvous guide à travers ces étapes. Ces parcs commencent par une file d'attente et une flotte automatiquement associées. Cette approche est un moyen pratique de créer des fermes de type bac à sable dans lesquelles expérimenter.

Rubriques

- Configurez votre Compte AWS
- Configurer le moniteur Deadline Cloud
- Configuration d'un poste de développement pour Deadline Cloud
- Configurer les soumissionnaires de Deadline Cloud
- Utilisez la ferme

Configurez votre Compte AWS

Configurez votre compte Compte AWS pour utiliser AWS Deadline Cloud.

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

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

2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte.

> **Important**
>
> Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Configurer le moniteur Deadline Cloud

Pour commencer, vous devez créer votre infrastructure de surveillance Deadline Cloud et définir votre ferme. Vous pouvez également effectuer des étapes facultatives supplémentaires, notamment ajouter des groupes et des utilisateurs, choisir un rôle de service et ajouter des balises à vos ressources.

Étape 1 : configurer votre moniteur

Le moniteur Deadline Cloud est utilisé AWS IAM Identity Center pour autoriser les utilisateurs. L'instance IAM Identity Center que vous utilisez pour Deadline Cloud doit être Région AWS identique

à celle du moniteur. Si votre console utilise une autre région lorsque vous créez le moniteur, vous recevrez un rappel vous demandant de passer à la région du centre d'identité IAM.

L'infrastructure de votre moniteur comprend les composants suivants :

- Nom d'affichage du moniteur : le nom d'affichage du moniteur permet d'identifier votre moniteur, par exemple un AnyCompany moniteur. Le nom de votre moniteur détermine également l'URL de votre moniteur.

  > **Important**
  >
  > Vous ne pouvez pas modifier le nom d'affichage du moniteur une fois la configuration terminée.

- URL du moniteur : vous pouvez accéder à votre moniteur à l'aide de l'URL du moniteur. L'URL est basée sur le nom d'affichage du moniteur, par exemple https://anycompanymonitor.awsapps.com.

  > **Important**
  >
  > Vous ne pouvez pas modifier l'URL du moniteur une fois la configuration terminée.

- Région AWS: Région AWSIl s'agit de l'emplacement physique d'un ensemble de centres de AWS données. Lorsque vous configurez votre moniteur, la région utilise par défaut l'emplacement le plus proche de chez vous. Nous vous recommandons de changer de région afin qu'elle soit la plus proche de vos utilisateurs. Cela réduit le décalage et améliore les vitesses de transfert de données. AWS IAM Identity Center doit être activé de la même manière Région AWS que Deadline Cloud.

  > **Important**
  >
  > Vous ne pouvez pas changer de région une fois que vous avez terminé de configurer Deadline Cloud.

Effectuez les tâches décrites dans cette section pour configurer l'infrastructure de votre moniteur.

Pour configurer l'infrastructure de votre moniteur

1. Connectez-vous au pour démarrer la configuration AWS Management Consolede Welcome to Deadline Cloud, puis choisissez Next.

2. Entrez le nom d'affichage du moniteur, par exemple**`AnyCompany Monitor`**.
3. (Facultatif) Pour modifier le nom du moniteur, choisissez Modifier l'URL.
4. (Facultatif) Pour modifier la Région AWSzone la plus proche de vos utilisateurs, choisissez Changer de région.

   a. Sélectionnez la région la plus proche de vos utilisateurs.

   b. Choisissez Appliquer la région.

   - (Facultatif) Pour ajouter des groupes et des utilisateurs, sélectionnez (Facultatif) Ajoutez des groupes et des utilisateurs.
   - (Facultatif) Pour personnaliser davantage la configuration de votre moniteur, sélectionnez Réglages supplémentaires.
5. Si vous êtes prêt Étape 2 : définir les détails de la ferme, choisissez Next.

(Facultatif) Ajoutez des groupes et des utilisateurs

Avant de terminer la configuration du moniteur Deadline Cloud, vous pouvez ajouter des utilisateurs du moniteur et les ajouter à un groupe.

Une fois la configuration terminée, vous pouvez créer de nouveaux utilisateurs et groupes, et gérer les utilisateurs, par exemple en leur attribuant des groupes, des autorisations et des applications, ou en supprimant des utilisateurs de votre moniteur.

Réglages supplémentaires

La configuration de Deadline Cloud inclut des paramètres supplémentaires. Grâce à ces paramètres, vous pouvez consulter toutes les modifications apportées par la configuration de Deadline Cloud à votre compte Compte AWS, configurer votre rôle d'utilisateur de surveillance et modifier le type de clé de chiffrement.

AWS IAM Identity Center

AWS IAM Identity Center est un service d'authentification unique basé sur le cloud pour la gestion des utilisateurs et des groupes. IAM Identity Center peut également être intégré à votre fournisseur d'authentification unique (SSO) d'entreprise afin que les utilisateurs puissent se connecter avec leur compte d'entreprise.

Deadline Cloud active IAM Identity Center par défaut, et il est nécessaire pour configurer et utiliser Deadline Cloud. L'instance IAM Identity Center que vous utilisez pour Deadline Cloud doit être Région AWS identique à celle du moniteur. Pour plus d'informations, reportez-vous à la section Qu'est-ce que c'est AWS IAM Identity Center.

Configurer le rôle d'accès au service

Un AWS service peut assumer un rôle de service pour effectuer des actions en votre nom. Deadline Cloud nécessite un rôle d'utilisateur de moniteur pour permettre aux utilisateurs d'accéder aux ressources de votre moniteur.

Vous pouvez associer des politiques gérées AWS Identity and Access Management (IAM) au rôle d'utilisateur du moniteur. Les politiques permettent aux utilisateurs d'effectuer certaines actions, telles que la création d'emplois dans une application Deadline Cloud spécifique. Comme les applications dépendent de conditions spécifiques définies dans la stratégie gérée, si vous n'utilisez pas les politiques gérées, l'application risque de ne pas fonctionner comme prévu.

Vous pouvez modifier le rôle de l'utilisateur du moniteur une fois la configuration terminée, à tout moment. Pour plus d'informations sur les rôles des utilisateurs, consultez la section Rôles IAM.

Les onglets suivants contiennent des instructions pour deux cas d'utilisation différents. Pour créer et utiliser un nouveau rôle de service, choisissez l'onglet Nouveau rôle de service. Pour utiliser un rôle de service existant, choisissez l'onglet Rôle de service existant.

New service role

Pour créer et utiliser un nouveau rôle de service

1. Sélectionnez Créer et utiliser un nouveau rôle de service.
2. (Facultatif) Entrez un nom de rôle d'utilisateur du service.
3. Choisissez Afficher les détails des autorisations pour plus d'informations sur le rôle.

Existing service role

Pour utiliser un rôle de service existant

1. Sélectionnez Utiliser un rôle de service existant.
2. Ouvrez la liste déroulante pour choisir un rôle de service existant.
3. (Facultatif) Choisissez Afficher dans la console IAM pour plus d'informations sur le rôle.

Étape 2 : définir les détails de la ferme

De retour sur la console Deadline Cloud, suivez les étapes suivantes pour définir les détails de la ferme.

1. Dans Détails de la ferme, ajoutez le nom de la ferme.
2. Dans Description, entrez la description de la ferme. Une description claire peut vous aider à identifier rapidement l'objectif de votre exploitation.
3. (Facultatif) Par défaut, vos données sont cryptées à l'aide d'une clé qui AWS détient et gère votre sécurité. Vous pouvez choisir Personnaliser les paramètres de chiffrement (avancés) pour utiliser une clé existante ou pour en créer une nouvelle que vous gérez.

   Si vous choisissez de personnaliser les paramètres de chiffrement à l'aide de la case à cocher, entrez un AWS KMS ARN ou créez-en un nouveau AWS KMS en choisissant Créer une nouvelle clé KMS.
4. (Facultatif) Choisissez Ajouter un nouveau tag pour ajouter un ou plusieurs tags à votre ferme.
5. Choisissez l'une des options suivantes :

   - Sélectionnez Passer à la révision et Créer pour revoir et créer votre ferme.
   - Sélectionnez Suivant pour passer à d'autres étapes facultatives.

(Facultatif) Étape 3 : définir les détails de la file d'attente

La file d'attente est chargée de suivre la progression et de planifier le travail pour vos tâches.

1. À partir de la section Détails de la file d'attente, indiquez un nom pour la file d'attente.
2. Dans Description, entrez la description de la file d'attente. Une description claire peut vous aider à identifier rapidement l'objectif de votre file d'attente.
3. Pour les pièces jointes aux Job, vous pouvez créer un nouveau compartiment Amazon S3 ou choisir un compartiment Amazon S3 existant. Si vous ne possédez pas de compartiment Amazon S3 existant, vous devez en créer un.

   a. Pour créer un nouveau compartiment Amazon S3, sélectionnez Créer un nouveau compartiment de tâches. Vous pouvez définir le nom du job bucket dans le champ Préfixe racine. Nous vous recommandons d'appeler le bucket**`deadlinecloud-job-attachments-[MONITORNAME]`**.

Vous ne pouvez utiliser que des lettres minuscules et des tirets. Pas d'espaces ni de caractères spéciaux.

b. Pour rechercher et sélectionner un compartiment Amazon S3 existant, sélectionnez Choisir parmi un compartiment Amazon S3 existant. Recherchez ensuite un compartiment existant en choisissant Browse S3. Lorsque la liste de vos compartiments Amazon S3 disponibles s'affiche, sélectionnez le compartiment Amazon S3 que vous souhaitez utiliser pour votre file d'attente.

4. Si vous utilisez des flottes gérées par le client, sélectionnez Activer l'association avec les flottes gérées par le client.

   - Pour les flottes gérées par le client, ajoutez un utilisateur configuré en file d'attente, puis définissez les informations d'identification POSIX et/ou Windows. Vous pouvez également contourner la fonctionnalité d'exécution en tant que telle en cochant la case.

5. Votre file d'attente nécessite une autorisation pour accéder à Amazon S3 en votre nom. Nous vous recommandons de créer un nouveau rôle de service pour chaque file d'attente.

   a. Pour un nouveau rôle, procédez comme suit.

      i. Sélectionnez Créer et utiliser un nouveau rôle de service.

      ii. Entrez un nom de rôle pour votre rôle de file d'attente ou utilisez le nom de rôle fourni.

      iii. (Facultatif) Ajoutez une description du rôle de file d'attente.

      iv. Vous pouvez consulter les autorisations IAM pour le rôle de file d'attente en choisissant Afficher les détails des autorisations.

   b. Vous pouvez également choisir un rôle de service existant.

6. (Facultatif) Ajoutez des variables d'environnement pour l'environnement de file d'attente à l'aide de paires de nom et de valeur.

7. (Facultatif) Ajoutez des balises pour la file d'attente à l'aide de paires clé/valeur.

Après avoir saisi tous les détails de la file d'attente, sélectionnez Suivant.

(Facultatif) Étape 4 : définir les détails de la flotte

Une flotte affecte des travailleurs pour exécuter vos tâches de rendu. Si vous avez besoin d'une flotte pour vos tâches de rendu, cochez la case Créer une flotte.

1. Détails de la flotte

a. Fournissez à la fois un nom et une description facultative pour votre flotte.

b. Sélectionnez la manière dont vos ressources informatiques doivent évoluer. L'option de gestion des services permet à Deadline Cloud de dimensionner automatiquement vos ressources informatiques. L'option gérée par le client vous permet de contrôler vous-même le dimensionnement de vos calculs.

2. Dans la section des options Instance, choisissez Spot ou On-Demand. Les instances Amazon EC2 On-Demand offrent une disponibilité plus rapide et les instances Amazon EC2 Spot sont idéales pour réduire les coûts.

3. Pour le dimensionnement automatique du nombre d'instances de votre parc, choisissez à la fois un nombre minimum d'instances et un nombre maximum d'instances.

   Nous vous recommandons vivement de toujours définir le nombre minimum d'instances **0** afin d'éviter des coûts supplémentaires.

4. Votre flotte a besoin d'une autorisation pour écrire CloudWatch en votre nom. Nous vous recommandons de créer un nouveau rôle de service pour chaque flotte.

   a. Pour un nouveau rôle, procédez comme suit.

      i. Sélectionnez Créer et utiliser un nouveau rôle de service.

      ii. Entrez un nom de rôle pour votre rôle dans la flotte ou utilisez le nom de rôle fourni.

      iii. (Facultatif) Ajoutez une description du rôle de la flotte.

      iv. Vous pouvez consulter les autorisations IAM associées au rôle de flotte en choisissant Afficher les détails des autorisations.

   b. Vous pouvez également utiliser un rôle de service existant.

5. (Facultatif) Ajoutez des balises pour la flotte à l'aide de paires clé/valeur.

Après avoir saisi tous les détails de la flotte, sélectionnez Suivant.

(Facultatif) Étape 5 : Configuration des exigences du travailleur

Définissez les exigences relatives à vos instances de travail.

1. Vérifiez les paramètres du système d'exploitation (OS) et de l'architecture du processeur pour en prendre connaissance.

2. Mettez à jour le nombre minimum et maximum de vCPU en fonction de vos exigences matérielles.
3. Mettez à jour le nombre minimum et maximum de mémoire (GiB) en fonction de vos exigences matérielles.
4. Vous pouvez filtrer les types d'instances en autorisant ou en excluant les types d'instances de travail. Dans les deux options de filtrage, vous pouvez filtrer jusqu'à 10 types d'instances Amazon EC2.
5. Sous Exigences supplémentaires (facultatif), vous pouvez définir le volume EBS racine par taille (GiB), IOPS et débit (MiB/s).
6. Une fois que toutes les exigences relatives au personnel sont définies, choisissez Next pour définir le niveau d'accès de vos groupes.

(Facultatif) Étape 6 : définir les niveaux d'accès

Si des groupes sont connectés à votre moniteur, vous pouvez définir leur niveau d'accès. L'autorisation d'utiliser les fonctionnalités de Deadline Cloud est gérée par niveaux d'accès. Vous pouvez attribuer différents niveaux d'accès à des groupes d'utilisateurs.

1. Utilisez le menu des niveaux d'accès à la ferme Deadline Cloud pour sélectionner le niveau d'autorisation du groupe.
2. Cliquez sur Suivant pour continuer et passer en revue tous les détails de la ferme saisis.

Étape 7 : Réviser et créer

Passez en revue toutes les informations saisies pour créer votre ferme. Lorsque vous êtes prêt, choisissez Create farm.

La progression de la création de votre ferme est affichée sur la page Fermes. Un message de réussite s'affiche lorsque votre ferme est prête à être utilisée.

Configuration d'un poste de développement pour Deadline Cloud

Dans ce didacticiel, vous allez AWS CloudShell créer une ferme de développement simple et exécuter l'agent de travail. Vous pouvez ensuite soumettre et exécuter une tâche simple avec des paramètres et des pièces jointes, ajouter un parc géré par des services et nettoyer les ressources de votre ferme lorsque vous avez terminé.

Les sections suivantes vous présentent les différentes fonctionnalités de Deadline Cloud, ainsi que leur fonctionnement et leur complémentarité. Il est utile de suivre ces étapes pour développer et tester de nouvelles charges de travail et personnalisations.

Rubriques

Étape 1 : Création d'un parc Deadline Cloud

Pour créer votre parc de développeurs et vos ressources de file d'attente dans AWS Deadline Cloud, utilisez le AWS Command Line Interface (AWS CLI), comme indiqué dans la procédure suivante. Vous allez également créer un rôle AWS Identity and Access Management (IAM) et une flotte gérée par le client (CMF) et associer la flotte à votre file d'attente. Vous pouvez ensuite configurer AWS CLI et confirmer que votre ferme est configurée et fonctionne comme indiqué.

Vous pouvez utiliser cette ferme pour explorer les fonctionnalités de Deadline Cloud, puis développer et tester de nouvelles charges de travail, personnalisations et intégrations de pipelines.

Pour créer une ferme

1. Installez et configurez le AWS Command Line Interface (AWS CLI), si ce n'est pas déjà fait. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.
2. Créez un nom pour votre ferme et ajoutez-y le nom de la ferme à`~/.bashrc`. Cela le rendra disponible pour les autres sessions du terminal.

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

3. Créez la ressource agricole et ajoutez-y son identifiant de ferme`~/.bashrc`.

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

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

4. Créez la ressource de file d'attente et ajoutez son ID de file d'attente à `~/.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. Créez un rôle IAM pour la flotte. Ce rôle fournit aux travailleurs hôtes de votre flotte les informations d'identification de sécurité nécessaires pour exécuter des tâches depuis votre file d'attente.

```
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. Créez la flotte gérée par le client (CMF) et ajoutez son identifiant de flotte à`~/.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. Assurez-vous que vous pouvez accéder à Deadline Cloud.

```
pip install deadline
```

8. Associez le CMF à votre file d'attente.

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

9. Pour définir le parc par défaut sur l'ID du parc de serveurs et la file d'attente sur l'ID de file d'attente que vous avez créé précédemment, utilisez la commande suivante.

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

10. (Facultatif) Pour vérifier que votre ferme est configurée conformément à vos spécifications, utilisez les commandes suivantes :

    - Liste de toutes les fermes — **`deadline farm list`**
    - Répertorier toutes les files d'attente de la ferme par défaut — **`deadline queue list`**
    - Répertorier toutes les flottes de la ferme par défaut : **`deadline fleet list`**
    - Obtenez la ferme par défaut — **`deadline farm get`**
    - Obtenez la file d'attente par défaut — **`deadline queue get`**
    - Obtenez toutes les flottes associées à la file d'attente par défaut — **`deadline fleet get`**

Étape 2 : Exécuter l'agent de travail en mode développeur dans Deadline Cloud

Avant de pouvoir exécuter les tâches que vous soumettez à la file d'attente de votre parc de développeurs, vous devez exécuter l'agent de travail de AWS Deadline Cloud en mode développeur sur un hôte de travail.

Dans le reste de ce didacticiel, vous allez effectuer des AWS CLI opérations sur votre ferme de développeurs à l'aide de deux AWS CloudShell onglets. Dans le premier onglet, vous pouvez soumettre des offres d'emploi. Dans le deuxième onglet, vous pouvez exécuter l'agent de travail.

> **Note**
>
> Si vous laissez votre CloudShell session inactive pendant plus de 20 minutes, le délai expirera et l'agent de travail sera arrêté. Pour redémarrer l'agent de travail, suivez les instructions de la procédure suivante.

Pour exécuter l'agent de travail en mode développeur

1. Installez et configurez le AWS Command Line Interface (AWS CLI), si ce n'est pas déjà fait. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.
2. Votre ferme étant toujours ouverte dans le premier CloudShell onglet, ouvrez un deuxième CloudShell onglet, puis créez les `demoenv-persist` répertoires `demoenv-logs` et.

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

3. Téléchargez et installez les packages d'agents de travail de Deadline Cloud depuis PyPI :

> **Note**
>
> WindowsActivé, les fichiers de l'agent doivent être installés dans le répertoire global site-packages de Python. Les environnements virtuels Python ne sont actuellement pas pris en charge.

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

4. Pour permettre à l'agent de travail de créer les répertoires temporaires pour exécuter les tâches, créez un répertoire :

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

5. Exécutez l'agent de travail de Deadline Cloud en mode développeur avec les variables `DEV_FARM_ID` et `DEV_CMF_ID` celles que vous avez ajoutées au`~/.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
```

Lorsque l'agent de travail initialise puis interroge l'opération d'`UpdateWorkerSchedule`API, le résultat suivant s'affiche :

```
INFO    Worker Agent starting
[2024-03-27 15:51:01,292][INFO    ] # Worker Agent starting
[2024-03-27 15:51:01,292][INFO    ] AgentInfo
Python Interpreter: /usr/bin/python3
Python Version: 3.9.16 (main, Sep  8 2023, 00:00:00)  - [GCC 11.4.1 20230605 (Red
 Hat 11.4.1-2)]
Platform: linux
...
[2024-03-27 15:51:02,528][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params={'assignedSessions': {}, 'cancelSessionActions': {},
 'updateIntervalSeconds': 15} ...
[2024-03-27 15:51:17,635][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params=(Duplicate removed, see previous response) ...
[2024-03-27 15:51:32,756][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params=(Duplicate removed, see previous response) ...
...
```

6. Sélectionnez votre premier CloudShell onglet, puis listez les travailleurs de la flotte.

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

Des résultats tels que les suivants sont affichés :

```
Displaying 1 of 1 workers starting at 0

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

Dans une configuration de production, l'agent de travail de Deadline Cloud nécessite la configuration de plusieurs utilisateurs et répertoires de configuration en tant qu'utilisateur administratif sur la machine hôte. Vous pouvez annuler ces paramètres car vous exécutez des tâches dans votre propre ferme de développement, à laquelle vous seul pouvez accéder.

Étape 3 : Soumettre et exécuter des tâches avec Deadline Cloud

Pour utiliser AWS Deadline Cloud pour exécuter des tâches, suivez les procédures suivantes. Utilisez le premier AWS CloudShell onglet pour soumettre des offres d'emploi à votre parc de développeurs. Utilisez le deuxième CloudShell onglet pour afficher la sortie de l'agent de travail.

Rubriques

Soumettre l'simple_jobéchantillon

Après avoir créé une ferme et exécuté l'agent de travail, vous pouvez envoyer l'simple_jobéchantillon à Deadline Cloud.

Pour envoyer l'simple_jobéchantillon à Deadline Cloud

1. Installez et configurez le AWS Command Line Interface (AWS CLI), si ce n'est pas déjà fait. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.
2. Téléchargez l'exemple à partir de GitHub.

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

3. Choisissez votre premier CloudShell onglet, puis accédez au répertoire des exemples de lots de tâches.

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

4. Soumettez l'simple_jobéchantillon.

```
deadline bundle submit simple_job
```

5. Choisissez votre deuxième CloudShell onglet pour afficher les résultats de journalisation concernant les appels`BatchGetJobEntities`, l'obtention d'une session et l'exécution d'une action de session.

```
...
[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**
>
> Seule la sortie de journalisation de l'agent de travail est affichée. Il existe un journal distinct pour la session qui exécute le travail.

6. Choisissez votre premier onglet, puis inspectez les fichiers journaux écrits par l'agent de travail.

a. Accédez au répertoire des journaux de l'agent de travail et visualisez son contenu.

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

b. Imprimez le premier fichier journal créé par l'agent de travail.

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

Ce fichier contient une sortie de l'agent de travail expliquant comment il a appelé l'API Deadline Cloud pour créer une ressource de personnel dans votre flotte, puis a assumé le rôle de flotte.

c. Imprimez la sortie du fichier journal lorsque l'agent des travailleurs rejoint le parc.

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

Ce journal contient des résultats sur toutes les actions effectuées par l'agent de travail, mais pas sur les files d'attente à partir desquelles il exécute les tâches, à l'exception des identifiants de ces ressources.

d. Imprimez les fichiers journaux de chaque session dans un répertoire dont le nom est identique à l'identifiant de la ressource de file d'attente.

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

En cas de réussite de la tâche, le résultat du fichier journal sera similaire à ce qui suit :

```
 cat $DEV_QUEUE_ID/$(ls -t $DEV_QUEUE_ID | head -1)
2024-03-27 16:00:22,026 WARNING Session running with no AWS Credentials.
2024-03-27 16:00:22,404 INFO
2024-03-27 16:00:22,405 INFO ================================================
2024-03-27 16:00:22,405 INFO --------- Running Task
2024-03-27 16:00:22,405 INFO ================================================
2024-03-27 16:00:22,406 INFO ------------------------------------------------
2024-03-27 16:00:22,406 INFO Phase: Setup
2024-03-27 16:00:22,406 INFO ------------------------------------------------
2024-03-27 16:00:22,406 INFO Writing embedded files for Task to disk.
2024-03-27 16:00:22,406 INFO Mapping: Task.File.runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_fileswa_gj55_/tmp2u9yqtsz
```

```
2024-03-27 16:00:22,406 INFO Wrote: runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_fileswa_gj55_/tmp2u9yqtsz
2024-03-27 16:00:22,407 INFO ------------------------------------------------
2024-03-27 16:00:22,407 INFO Phase: Running action
2024-03-27 16:00:22,407 INFO ------------------------------------------------
2024-03-27 16:00:22,407 INFO Running command /sessions/
session-053d77cef82648fea9c698271812a/tmpzuzxpslm.sh
2024-03-27 16:00:22,414 INFO Command started as pid: 471
2024-03-27 16:00:22,415 INFO Output:
2024-03-27 16:00:22,420 INFO Welcome to AWS Deadline Cloud!
2024-03-27 16:00:22,571 INFO
2024-03-27 16:00:22,572 INFO ================================================
2024-03-27 16:00:22,572 INFO --------- Session Cleanup
2024-03-27 16:00:22,572 INFO ================================================
2024-03-27 16:00:22,572 INFO Deleting working directory: /sessions/
session-053d77cef82648fea9c698271812a
```

7. Imprimez les informations relatives à la tâche.

   ```
   deadline job get
   ```

   Lorsque vous soumettez la tâche, le système l'enregistre par défaut afin que vous n'ayez pas à saisir l'ID de la tâche.

Soumettre un simple_job avec un paramètre

Vous pouvez soumettre des tâches avec des paramètres. Dans la procédure suivante, vous modifiez le simple_job modèle pour inclure un message personnalisé, vous soumettez le fichier journal de sessionsimple_job, puis vous l'imprimez pour afficher le message.

Pour soumettre l'simple_jobéchantillon avec un paramètre

1. Sélectionnez votre premier CloudShell onglet, puis accédez au répertoire des exemples de lots de tâches.

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

2. Imprimez le contenu du simple_job modèle.

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

La `parameterDefinitions` section contenant le `Message` paramètre doit ressembler à ce qui suit :

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

3. Soumettez l'simple_jobexemple avec une valeur de paramètre, puis attendez que le travail soit terminé.

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

4. Pour voir le message personnalisé, consultez le fichier journal de session le plus récent.

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

Création d'un ensemble de tâches simple_file_job avec des E/S de fichiers

Une tâche de rendu doit lire la définition de la scène, en faire le rendu d'une image, puis enregistrer cette image dans un fichier de sortie. Vous pouvez simuler cette action en demandant à la tâche de calculer le hachage de l'entrée au lieu de restituer une image.

Pour créer un ensemble de tâches simple_file_job avec des E/S de fichiers

1. Sélectionnez votre premier CloudShell onglet, puis accédez au répertoire des exemples de lots de tâches.

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

2. Faites-en une copie `simple_job` avec le nouveau nom`simple_file_job`.

```
cp -r simple_job simple_file_job
```

3. Modifiez le modèle de tâche comme suit :

> **Note**
>
> Nous vous recommandons de l'utiliser nano pour ces étapes. Si vous préférez l'utiliserVim, vous devez définir son mode de collage à l'aide de`:set paste`.

a. Ouvrez le modèle dans un éditeur de texte.

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

b. Ajoutez les éléments suivants `typeobjectType`, et `dataFlowparameterDefinitions`.

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

c. Ajoutez la commande de `bash` script suivante à la fin du fichier qui lit le fichier d'entrée et écrit dans le fichier de sortie.

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

La mise à jour `template.yaml` doit correspondre exactement à ce qui suit :

```
specificationVersion: 'jobtemplate-2023-09'
name: Simple File Job Bundle Example
parameterDefinitions:
- name: Message
  type: STRING
  default: Welcome to AWS Deadline Cloud!
- name: InFile
  type: PATH
  objectType: FILE
  dataFlow: IN
- name: OutFile
```

```
  type: PATH
  objectType: FILE
  dataFlow: OUT
steps:
- name: WelcomeToDeadlineCloud
  script:
    actions:
      onRun:
        command: '{{Task.File.runScript}}'
    embeddedFiles:
    - name: runScript
      type: TEXT
      runnable: true
      data: |
        #!/usr/bin/env bash
        echo "{{Param.Message}}"

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

> **Note**
>
> Si vous souhaitez ajuster l'espacement dans le`template.yaml`, assurez-vous d'utiliser des espaces plutôt que des indentations.

d. Enregistrez le fichier et quittez l'éditeur de texte.

4. Fournissez des valeurs de paramètres pour les fichiers d'entrée et de sortie afin de soumettre le simple_file_job.

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

5. Imprimez les informations relatives à la tâche.

```
deadline job get
```

- Vous verrez des résultats tels que les suivants :

```
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
```

- Bien que vous n'ayez fourni que des chemins relatifs, le chemin complet est défini pour les paramètres. AWS CLI joint le répertoire de travail actuel à tous les chemins fournis en tant que paramètres lorsque les chemins ont le typePATH.
- L'agent de travail exécuté dans l'autre fenêtre du terminal prend en charge et exécute la tâche. Cette action crée le `hash.txt` fichier, que vous pouvez consulter à l'aide de la commande suivante.

  ```
  cat hash.txt
  ```

  Cette commande imprime une sortie similaire à la suivante.

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

Étape 4 : Exécuter des tâches avec des pièces jointes dans Deadline Cloud

De nombreuses fermes utilisent des systèmes de fichiers partagés pour partager des fichiers entre les hôtes qui soumettent des tâches et ceux qui exécutent des tâches. Par exemple, dans l'`simple_file_job`exemple précédent, le système de fichiers local est partagé entre les fenêtres du AWS CloudShell terminal, qui s'exécutent dans l'onglet 1 où vous soumettez le travail, et dans l'onglet 2 où vous exécutez l'agent de travail.

Un système de fichiers partagé est avantageux lorsque le poste de travail émetteur et les hôtes de travail se trouvent sur le même réseau local. Si vous stockez vos données sur site à proximité des postes de travail qui y accèdent, l'utilisation d'une ferme basée sur le cloud signifie que vous devez partager vos systèmes de fichiers via un VPN à latence élevée ou synchroniser vos systèmes de fichiers dans le cloud. Aucune de ces options n'est facile à configurer ou à utiliser.

AWS Deadline Cloud propose une solution simple avec des pièces jointes à des tâches, similaires à des pièces jointes à des e-mails. Avec les pièces jointes à une tâche, vous associez des données à

votre tâche. Deadline Cloud gère ensuite les détails du transfert et du stockage de vos données de travail dans des compartiments Amazon Simple Storage Service (Amazon S3).

Les processus de création de contenu sont souvent itératifs, ce qui signifie qu'un utilisateur soumet des tâches avec un petit sous-ensemble de fichiers modifiés. Comme les compartiments Amazon S3 stockent les pièces jointes aux tâches dans un espace de stockage adressable par le contenu, le nom de chaque objet est basé sur le hachage des données de l'objet et le contenu d'une arborescence de répertoires est stocké dans un format de fichier manifeste joint à une tâche.

Pour exécuter des tâches avec des pièces jointes, procédez comme suit.

Rubriques

- Ajoutez une configuration de pièces jointes aux tâches à votre file d'attente
- Soumettre simple_file_job avec des pièces jointes
- Comprendre comment les pièces jointes aux tâches sont stockées dans Amazon S3

Ajoutez une configuration de pièces jointes aux tâches à votre file d'attente

Pour activer les pièces jointes aux tâches dans votre file d'attente, ajoutez une configuration de pièces jointes aux tâches à la ressource de file d'attente de votre compte.

Pour ajouter une configuration de pièces jointes aux tâches à votre file d'attente

1. Installez et configurez le AWS Command Line Interface (AWS CLI), si ce n'est pas déjà fait. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.
2. Choisissez votre premier CloudShell onglet, puis entrez l'une des commandes suivantes pour utiliser un compartiment Amazon S3 pour les pièces jointes aux tâches.
   - Si vous n'avez pas de compartiment Amazon S3 privé existant, vous pouvez créer et utiliser un nouveau compartiment 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}
```

- Si vous possédez déjà un compartiment Amazon S3 privé, vous pouvez l'utiliser en le *MY_BUCKET_NAME*remplaçant par le nom de votre compartiment.

```
DEV_FARM_BUCKET=MY_BUCKET_NAME
```

3. Après avoir créé ou choisi votre compartiment Amazon S3, ajoutez le nom du compartiment `~/.bashrc` pour le rendre disponible pour d'autres sessions de terminal.

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

4. Créez un rôle AWS Identity and Access Management (IAM) pour la file d'attente.

```
aws iam create-role --role-name "${DEV_FARM_NAME}QueueRole" \
    --assume-role-policy-document \
        '{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "credentials.deadline.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }'
aws iam put-role-policy \
    --role-name "${DEV_FARM_NAME}QueueRole" \
    --policy-name S3BucketsAccess \
    --policy-document \
            '{
                "Version": "2012-10-17",
                "Statement": [
                {
                    "Action": [
                        "s3:GetObject*",
                        "s3:GetBucket*",
                        "s3:List*",
                        "s3:DeleteObject*",
                        "s3:PutObject",
                        "s3:PutObjectLegalHold",
```

```
                    "s3:PutObjectRetention",
                    "s3:PutObjectTagging",
                    "s3:PutObjectVersionTagging",
                    "s3:Abort*"
                ],
                "Resource": [
                    "arn:aws:s3:::'$DEV_FARM_BUCKET'",
                    "arn:aws:s3:::'$DEV_FARM_BUCKET'/*"
                ],
                "Effect": "Allow"
            }
        ]
        }'
```

5. Mettez à jour votre file d'attente pour inclure les paramètres des pièces jointes aux tâches et le rôle 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. Confirmez que vous avez mis à jour votre file d'attente.

```
deadline queue get
```

Des résultats tels que les suivants sont affichés :

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

Soumettre simple_file_job avec des pièces jointes

Lorsque vous utilisez des pièces jointes à des tâches, les ensembles de tâches doivent fournir à Deadline Cloud suffisamment d'informations pour déterminer le flux de données de la tâche, par exemple en utilisant des PATH paramètres. Dans ce cassimple_file_job, vous avez modifié le `template.yaml` fichier pour indiquer à Deadline Cloud que le flux de données se trouve dans le fichier d'entrée et le fichier de sortie.

Après avoir ajouté la configuration des pièces jointes aux tâches à votre file d'attente, vous pouvez envoyer l'exemple simple_file_job avec les pièces jointes aux tâches. Ensuite, vous pouvez consulter le journal et le résultat de la tâche pour confirmer que les pièces jointes simple_file_job aux tâches fonctionnent.

Pour soumettre le bundle de tâches simple_file_job avec des pièces jointes

1. Choisissez votre premier CloudShell onglet, puis ouvrez le `JobBundle-Samples` répertoire.
2.
```
cd ~/AmazonDeadlineCloud-DocumentationAndSamples/JobBundle-Samples
```
3. Soumettez simple_file_job à la file d'attente. Lorsque vous êtes invité à confirmer le téléchargement, entrez**y**.

```
deadline bundle submit simple_file_job \
    -p InFile=simple_job/template.yaml \
    -p OutFile=hash-jobattachments.txt
```
4. Pour afficher les résultats du journal de session de transfert de données des pièces jointes aux tâches, choisissez le deuxième CloudShell onglet.

```
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. Répertoriez les actions de session exécutées au cours de la session.

```
aws deadline list-session-actions \
```

```
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --session-id $SESSION_ID
```

Des résultats tels que les suivants sont affichés :

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

La première action de session a téléchargé les pièces jointes des tâches d'entrée, tandis que la seconde a exécuté la tâche comme avant, puis a chargé les pièces jointes des tâches de sortie.

6. Répertoriez le répertoire de sortie.

```
ls *.txt
```

Une sortie telle que `hash.txt` celle qui est affichée, mais qui `hash-jobattachments.txt` n'existe pas.

7. Téléchargez le résultat de la tâche la plus récente.

```
deadline job download-output
```

8. Affichez le résultat du fichier téléchargé.

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

Des résultats tels que les suivants sont affichés :

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

Comprendre comment les pièces jointes aux tâches sont stockées dans Amazon S3

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour charger ou télécharger des données relatives aux pièces jointes aux tâches, qui sont stockées dans des compartiments Amazon S3. Comprendre comment Deadline Cloud stocke les pièces jointes aux tâches sur Amazon S3 vous aidera à développer des charges de travail et à intégrer des pipelines.

Pour vérifier comment les pièces jointes aux tâches de Deadline Cloud sont stockées dans Amazon S3

1. Choisissez votre premier CloudShell onglet, puis ouvrez le répertoire des exemples de lots de tâches.

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

2. Inspectez les propriétés de la tâche.

```
deadline job get
```

Des résultats tels que les suivants sont affichés :

```
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
```

Le champ Pièces jointes contient une liste de structures de manifeste qui décrivent les chemins de données d'entrée et de sortie utilisés par la tâche lors de son exécution. Regardez `rootPath` le chemin du répertoire local sur la machine qui a soumis le travail. Pour voir le suffixe d'objet Amazon S3 qui contient un fichier manifeste, consulte`inputManifestFile`. Le fichier manifeste contient des métadonnées pour un instantané de l'arborescence des répertoires des données d'entrée de la tâche.

3. Imprimez joliment l'objet manifeste Amazon S3 pour voir la structure du répertoire d'entrée correspondant à la tâche.

```
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 .
```

Des résultats tels que les suivants sont affichés :

```
{
```

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

4. Créez le préfixe Amazon S3 qui contient les manifestes pour les pièces jointes aux tâches de sortie et listez l'objet situé en dessous.

```
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
```

Les pièces jointes aux tâches de sortie ne sont pas directement référencées à partir de la ressource de travail, mais sont placées dans un compartiment Amazon S3 en fonction des identifiants des ressources de la ferme.

5. Obtenez la clé d'objet manifeste la plus récente pour l'identifiant d'action de session spécifique, puis imprimez joliment les objets du manifeste.

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

```
echo $MANIFEST_OBJECT | jq .
```

Vous verrez les propriétés du fichier `hash-jobattachments.txt` dans la sortie, telles que les suivantes :

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

Votre tâche ne comportera qu'un seul objet manifeste par exécution de tâche, mais en général, il est possible d'avoir plus d'objets par exécution de tâche.

6. Affichez la sortie de stockage Amazon S3 adressable au contenu sous le préfixe. `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 -
```

Des résultats tels que les suivants sont affichés :

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

Étape 5 : Ajoutez un parc géré par des services à votre parc de développeurs dans Deadline Cloud

AWS CloudShell ne fournit pas une capacité de calcul suffisante pour tester des charges de travail plus importantes. Il n'est pas non plus configuré pour fonctionner avec des tâches qui distribuent des tâches sur plusieurs hôtes de travail.

Au lieu de l'utiliser CloudShell, vous pouvez ajouter une flotte gérée par le service Auto Scaling (SMF) à votre parc de développeurs. Un SMF fournit une capacité de calcul suffisante pour des charges de travail plus importantes et peut gérer des tâches nécessitant de répartir les tâches entre plusieurs hôtes de travail. Le planificateur utilisera à la fois les travailleurs SMF et CMF pour exécuter les tâches, sauf si vous arrêtez le programme de travail CMF.

Pour ajouter un parc géré par des services à votre parc de développeurs

1. Installez et configurez le AWS Command Line Interface (AWS CLI), si ce n'est pas déjà fait. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.
2. Choisissez votre premier AWS CloudShell onglet, puis créez le parc géré par le service et ajoutez-y son identifiant de flotte`.bashrc`. Cette action le rend disponible pour d'autres sessions de terminal.

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

```
                },
                "instanceMarketOptions": {
                    "type": "spot"
                }
            }
        }'

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

3. Associez le SMF à votre file d'attente.

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

4.

> **Note**
>
> Le planificateur utilisera à la fois les travailleurs SMF et CMF pour exécuter les tâches, sauf si vous arrêtez le programme de travail CMF.

Soumettre simple_file_job à la file d'attente. Lorsque vous êtes invité à confirmer le téléchargement, entrez**y**.

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

5. Vérifiez que le SMF fonctionne correctement.

```
deadline fleet get
```

- Le travailleur peut mettre quelques minutes à démarrer.
- La `queueFleetAssociationsStatus` flotte gérée par le client et la flotte gérée par le service seront les suivantes`ACTIVE`.

- Le SMF `autoScalingStatus` passera de `GROWING` à. `STEADY`

Votre statut ressemblera à ce qui suit :

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

6. Consultez le journal de la tâche que vous avez soumise. Ce journal est stocké dans un journal dans Amazon CloudWatch Logs, et non dans le système de CloudShell fichiers.

```
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
```

Étape 6 : Nettoyez les ressources de votre ferme dans Deadline Cloud

Pour développer et tester de nouvelles charges de travail et de nouvelles intégrations de pipeline, vous pouvez continuer à utiliser le parc de développeurs Deadline Cloud que vous avez créé pour ce didacticiel. Si vous n'avez plus besoin de votre parc de développeurs, vous pouvez supprimer ses ressources, notamment la ferme, le parc, la file d'attente, les rôles AWS Identity and Access Management (IAM) et les journaux dans Amazon CloudWatch Logs. Après avoir supprimé ces ressources, vous devrez recommencer le didacticiel pour pouvoir les utiliser. Pour plus d'informations, consultez Configuration d'un poste de développement pour Deadline Cloud.

Pour assainir les ressources agricoles des développeurs

1. Installez et configurez le AWS Command Line Interface (AWS CLI), si ce n'est pas déjà fait. Pour plus d'informations, voir Installer ou mettre à jour vers la dernière version du AWS CLI.
2. Choisissez votre premier CloudShell onglet, puis arrêtez toutes les associations de files d'attente et de flottes pour votre file d'attente.

```
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. Répertoriez les associations de parcs de files d'attente.

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

Vous devrez peut-être réexécuter la commande jusqu'à ce que le résultat soit `"status": "STOPPED"` affiché, puis vous pourrez passer à l'étape suivante. Ce processus peut prendre plusieurs minutes.

```
{
    "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. Supprimez toutes les associations de files d'attente et de flottes pour votre file d'attente.

```
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. Supprimez toutes les flottes associées à votre file d'attente.

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

6. Supprimez la file d'attente.

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

7. Supprimez la ferme.

```
aws deadline delete-farm \
```

```
    --farm-id $DEV_FARM_ID
```

8. Supprimez les autres AWS ressources de votre ferme.

   a. Supprimez le rôle de flotte 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. Supprimez le rôle IAM de la file d'attente.

   ```
   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. Supprimez les groupes de CloudWatch journaux Amazon Logs. Chaque file d'attente et flotte possède son propre groupe de journaux.

   ```
   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"
   ```

Configurer les soumissionnaires de Deadline Cloud

Ce processus est destiné aux administrateurs et aux artistes qui souhaitent installer, configurer et lancer l'émetteur AWS Deadline Cloud. Un émetteur de Deadline Cloud est un plugin de création de contenu numérique (DCC). Les artistes l'utilisent pour soumettre des offres d'emploi à partir d'une interface DCC tierce qu'ils connaissent bien.

> **Note**
>
> Ce processus doit être effectué sur tous les postes de travail que les artistes utiliseront pour soumettre des rendus.

Rubriques

Étape 1 : Installation de l'émetteur Deadline Cloud

Les sections suivantes vous indiquent les étapes d'installation de l'émetteur Deadline Cloud.

Téléchargez le programme d'installation de l'émetteur

Avant de pouvoir installer l'émetteur Deadline Cloud, vous devez télécharger le programme d'installation de l'émetteur. Actuellement, le programme d'installation de Deadline Cloud Submitter prend uniquement en charge Windows et. Linux

1. Connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la.
2. Dans le volet de navigation latéral, sélectionnez Téléchargements.
3. Localisez la section du programme d'installation de Deadline Cloud Submitter.
4. Sélectionnez le programme d'installation du système d'exploitation de votre ordinateur, puis choisissez Télécharger.

(Facultatif) Vérifiez l'authenticité du logiciel téléchargé

Pour vérifier que le logiciel que vous avez téléchargé est authentique, suivez la procédure suivante pour l'un Windows ou l'autreLinux.

> **Note**
>
> Vous pouvez utiliser ces instructions pour vérifier d'abord le programme d'installation, puis vérifier le moniteur Deadline Cloud après l'avoir téléchargé dans la section suivante (étape 2).

Windows

Pour vérifier l'authenticité des fichiers que vous avez téléchargés, procédez comme suit.

1. Dans la commande suivante, *file* remplacez-le par le fichier que vous souhaitez vérifier. Par exemple, ***C:\PATH\TO\MY*****DeadlineCloudSubmitter-windows-x64-installer.exe** . Remplacez-le également *signtool-sdk-version* par la version du SignTool SDK installée. Par exemple, **10.0.22000.0**.

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

2. Par exemple, vous pouvez vérifier le fichier d'installation de l'expéditeur de Deadline Cloud en exécutant la commande suivante :

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

Linux

Pour vérifier l'authenticité des fichiers téléchargés, utilisez l'outil de ligne de gpg commande.

1. Importez la OpenPGP clé du programme d'installation de Deadline Cloud Submitter en exécutant la commande suivante :

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

   mQINBGX6GQsBEADduUtJgqSXI+q76O6fsFwEYKmbnlyL0xKvlq32EZuyv0otZo5L
   le4m5Gg52AzrvPvDiUTLooAlvYeozaYyirIGsK08Ydz0Ftdjroiuh/mw9JSJDJRI
   rnRn5yKet1JFezkjopA3pjsTBP6lW/mb1bDBDEwwwtH0x9lV7A03FJ9T7Uzu/qSh
   qO/UYdkafro3cPASvkqgDt2tCvURfBcUCAjZVFcLZcVD5iwXacxvKsxxS/e7kuVV
   I1+VGT8Hj8XzWYhjCZxOLZk/fvpYPMyEEujN0fYUp6RtMIXve0C9awwMCy5nBG2J
   eE2Ol5DsCpTaBd4Fdr3LWcSs8JFA/YfP9auL3NczOozPoVJt+fw8CBlVIXO0J7l5
   hvHDjcC+5v0wxqAlMG6+f/SX7CT8FXK+L3iOJ5gBYUNXqHSxUdv8kt76/KVmQa1B
   Akl+MPKpMq+lhw++S3G/lXqwWaDNQbRRw7dSZHymQVXvPp1nsqc3hV7KlOM+6s6g
   1g4mvFY4lf6DhptwZLWyQXU8rBQpojvQfiSmDFrFPWFi5BexesuVnkGIolQoklKx
   AVUSdJPVEJCteyy7td4FPhBaSqT5vW3+ANbr9b/uoRYWJvn17dN0cc9HuRh/Ai+I
   nkfECo2WUDLZ0fEKGjGyFX+todWvJXjvc5kmE9Ty5vJp+M9Vvb8jd6t+mwARAQAB
   tCxBV1MgRGVhZGxpbmUgQ2xvdWQgPGF3cy1kZWFkbGluZUBhbWF6b24uY29tPokC
   VwQTAQgAQRYhBLhAwIwpqQeWoHH6pfbNPOa3bzzvBQJl+hkLAxsvBAUJA8JnAAUL
   ```

```
CQgHAgIiAgYVCgkICwIDFgIBAh4HAheAAAoJEPbNPOa3bzzvKswQAJXzKSAY8sY8
F6Eas2oYwIDDdDurs8FiEnFghjUEO6MTt9AykF/jw+CQg2UzFtEyObHBymhgmhXE
3buVeom96tgM3ZDfZu+sxi5pGX6oAQnZ6riztN+VpkpQmLgwtMGpSMLl3KLwnv2k
WK8mrR/fPMkfdaewB7A6RIUYiW33GAL4KfMIs8/vIwIJw99NxHpZQVoU6dFpuDtE
1OuxGcCqGJ7mAmo6H/YawSNp2Ns80gyqIKYo7o3LJ+WRroIRlQyctq8gnR9JvYXX
42ASqLq5+OXKo4qh81blXKYqtc176BbbSNFjWnzIQgKDgNiHFZCdcOVgqDhwO15r
NICbqqwwNLj/Fr2kecYx180Ktpl0jOOw5IOyh3bf3MVGWnYRdjvA1v+/CO+55N4g
z0kf50Lcdu5RtqV10XBCifn28pecqPaSdYcssYSRl5DLiFktGbNzTGcZZwITTKQc
af8PPdTGtnnb6P+cdbW3bt9MVtN5/dgSHLThnS8MPEuNCtkTnpXshuVuBGgwBMdb
qUC+HjqvhZzbwns8dr5WI+6HWNBFgGANn6ageYl58vVp0UkuNP8wcWjRARciHXZx
ku6W2jPTHDWGNrBQO2Fx7fd2QYJheIPPAShHcfJO+xgWCof45D0vAxAJ8gGg9Eq+
gFWhsx4NSHn2gh1gDZ41Ou/4exJ1lwPM
=uVaX
-----END PGP PUBLIC KEY BLOCK-----
EOF
```

2. Déterminez s'il faut faire confiance à la 0penPGP clé. Certains facteurs à prendre en compte pour décider de faire confiance à la clé ci-dessus sont les suivants :

   - La connexion Internet que vous avez utilisée pour obtenir la clé GPG sur ce site Web est sécurisée.
   - L'appareil sur lequel vous accédez à ce site Web est sécurisé.
   - AWS a pris des mesures pour sécuriser l'hébergement de la clé 0penPGP publique sur ce site Web.

3. Si vous décidez de faire confiance à la OpenPGP clé, modifiez-la gpg comme dans l'exemple suivant :

```
$ 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. Vérifier le programme d'installation

   Pour vérifier le programme d'installation, procédez comme suit :

   a. Retournez à la page de téléchargement de la console Deadline Cloud et téléchargez le fichier de signature du programme d'installation de Deadline Cloud Submitter.

   b. Vérifiez la signature du programme d'installation de l'émetteur de Deadline Cloud en exécutant :

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

5. Vérifiez le moniteur Deadline Cloud

   > **Note**
   >
   > Vous pouvez vérifier le téléchargement du moniteur Deadline Cloud à l'aide de fichiers de signature ou de méthodes spécifiques à la plate-forme. Pour les

méthodes spécifiques à la plate-forme, consultez l'Linux (DEB)onglet ou l'Linux (AppImage)onglet en fonction du type de fichier que vous avez téléchargé.

Pour vérifier l'application de bureau Deadline Cloud Monitor avec les fichiers de signature, procédez comme suit :

a. Retournez à la page des téléchargements de la console Deadline Cloud et téléchargez le fichier .sig correspondant, puis exécutez

   Pour .deb :

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

   Pour. AppImage:

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

b. Vérifiez que le résultat ressemble à ce qui suit :

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

   gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
   ```

   Si la sortie contient cette phrase`Good signature from "AWS Deadline Cloud"`, cela signifie que la signature a été vérifiée avec succès et que vous pouvez exécuter le script d'installation du moniteur Deadline Cloud.

Linux (DEB)

Pour vérifier les packages qui utilisent un binaire Linux .deb, effectuez d'abord les étapes 1 à 3 de l'Linuxonglet.

dpkg est le principal outil de gestion de paquets dans la plupart des Linux distributions debian basées. Vous pouvez vérifier le fichier .deb à l'aide de l'outil.

1. Sur la page de téléchargement de la console Deadline Cloud, téléchargez le fichier .deb du moniteur Deadline Cloud.
2. ***<APP_VERSION>***Remplacez-le par la version du fichier .deb que vous souhaitez vérifier.

   ```
   dpkg-sig --verify deadline-cloud-monitor_<APP_VERSION>_amd64.deb
   ```
3. Le résultat sera similaire à :

   ```
   Processing deadline-cloud-monitor_1.1.1_amd64.deb... GOODSIG
   _gpgbuilder B840C08C29A90796A071FAA5F6CD3C 171200
   ```
4. Pour vérifier le fichier .deb, vérifiez qu'il GOODSIG est présent dans la sortie.

Linux (AppImage)

Pour vérifier les packages qui utilisent unLinux. AppImage binaire, commencez par effectuer les étapes 1 à 3 dans l'Linuxonglet.

1. Sur la page des téléchargements de la console Deadline Cloud, téléchargez le moniteur Deadline Cloud. AppImage fichier.
2. À <APP_VERSION>remplacer par la version du. AppImage fichier que vous souhaitez vérifier, procédez comme suit :

   a. Écrivez la signature à partir du. AppImage fichier dans un fichier .sig.

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

   b. Utilisez le fichier .sig généré pour vérifier à l'aide de la commande suivante.

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

   c. (Facultatif) Si une erreur d'autorisation refusée s'affiche, utilisez la commande suivante pour ajouter une autorisation d'exécution.

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

   d. Vérifiez que le résultat ressemble à ce qui suit :

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

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

Si la sortie contient cette phraseGood `signature from "AWS Deadline Cloud"`, cela signifie que la signature a été vérifiée avec succès et que vous pouvez exécuter le script d'installation du moniteur Deadline Cloud.

Installation de l'émetteur Deadline Cloud

Vous pouvez installer un émetteur Deadline Cloud avec Windows ou. Linux Avec le programme d'installation, vous pouvez installer les émetteurs suivants :

- Maya 2024
- Nuke 14,0 - 15,0
- Houdini 19,5
- Keyshot 12
- Mixeur 3.6
- Unreal Engine 5

Windows

1. Dans un navigateur de fichiers, accédez au dossier dans lequel le programme d'installation a été téléchargé, puis sélectionnez`DeadlineCloudSubmitter-windows-x64-installer.exe`.

   a. Si une fenêtre contextuelle protégée par Windows s'affiche, sélectionnez Plus d'informations.

   b. Choisissez tout de même Exécuter.
2. Lorsque l'assistant de configuration de AWS Deadline Cloud Submitter s'ouvre, choisissez Next.
3. Choisissez l'étendue de l'installation en effectuant l'une des étapes suivantes :
   - Pour effectuer l'installation uniquement pour l'utilisateur actuel, sélectionnez Utilisateur.
   - Pour effectuer l'installation pour tous les utilisateurs, sélectionnez Système.

Si vous choisissez Système, vous devez quitter le programme d'installation et le réexécuter en tant qu'administrateur en effectuant les étapes suivantes :

a. Cliquez avec le bouton droit sur**`DeadlineCloudSubmitter-windows-x64-installer.exe`**, puis choisissez Exécuter en tant qu'administrateur.

b. Entrez vos informations d'identification d'administrateur, puis choisissez Oui.

c. Choisissez System pour l'étendue de l'installation.

4. Après avoir sélectionné l'étendue de l'installation, choisissez Next.
5. Choisissez à nouveau Next pour accepter le répertoire d'installation.
6. Sélectionnez Émetteur intégré pour Nuke ou n'importe quel émetteur que vous souhaitez installer.
7. Choisissez Suivant.
8. Passez en revue l'installation, puis choisissez Next.
9. Cliquez à nouveau sur Suivant, puis sur Terminer.

Linux

> **Note**
>
> Le programme d'Nukeinstallation intégré de Deadline Cloud Linux et le moniteur Deadline Cloud ne peuvent être installés que sur Linux des distributions utilisant au moins la version GLIBC 2.31.

1. Ouvrez une fenêtre du terminal.
2. Pour effectuer une installation système du programme d'installation, entrez la commande **`sudo -i`** et appuyez sur Entrée pour devenir root.
3. Accédez à l'emplacement où vous avez téléchargé le programme d'installation.

   Par exemple, **`cd /home/`*`USER`*`/Downloads`**.
4. Pour rendre le programme d'installation exécutable, entrez**`chmod +x DeadlineCloudSubmitter-linux-x64-installer.run`**.
5. Pour exécuter le programme d'installation de Deadline Cloud Submitter, entrez. **`./DeadlineCloudSubmitter-linux-x64-installer.run`**

6. Lorsque le programme d'installation s'ouvre, suivez les instructions affichées à l'écran pour terminer l'assistant de configuration.

Vous pouvez installer d'autres émetteurs non répertoriés ici. Nous utilisons les bibliothèques Deadline Cloud pour créer des soumetteurs. Vous pouvez trouver le code source de ces bibliothèques et de ces émetteurs dans l'organisation GitHubaws-deadline.

Étape 2 : installer et configurer le moniteur Deadline Cloud

Vous pouvez installer l'application de bureau Deadline Cloud Monitor avec Windows ouLinux.

Windows

1. Si ce n'est pas déjà fait, connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la.
2. Dans le volet de navigation de gauche, sélectionnez Téléchargements.
3. Dans la section moniteur de Deadline Cloud, sélectionnez le fichier correspondant au système d'exploitation de votre ordinateur.
4. Pour télécharger le moniteur Deadline Cloud, choisissez Télécharger.

Linux

Pour installer le moniteur Deadline Cloud AppImage sur les distributions RPM

1. Téléchargez le dernier moniteur Deadline Cloud AppImage.
2. Pour rendre l' AppImage exécutable, entrez**`chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`**.
3. Pour configurer le chemin de certificat SSL correct, entrez**`sudo ln -sf /etc/ssl/certs/ca-bundle.crt /etc/ssl/certs/ca-certificates.crt`**.

Pour installer le moniteur Deadline Cloud AppImage sur les distributions Debian

1. Téléchargez le dernier moniteur Deadline Cloud AppImage.

2. > **Note**
   >
   > Cette étape concerne Ubuntu 22 et versions ultérieures. Pour les autres versions d'Ubuntu, ignorez cette étape.

   Pour installer libfuse2, entrez **`sudo apt udpate`**

   `sudo apt install libfuse2`.

3. Pour rendre l' AppImage exécutable, entrez**`chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`**.

Pour installer le paquet Debian Deadline Cloud monitor sur les distributions Debian

1. Téléchargez le dernier paquet Debian Deadline Cloud Monitor.
2. > **Note**
   >
   > Cette étape concerne Ubuntu 22 et versions ultérieures. Pour les autres versions d'Ubuntu, ignorez cette étape.

   Pour installer libssl1.1, entrez **`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. Pour installer le paquet Debian Deadline Cloud monitor, entrez **`sudo apt update`**

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

4. Si l'installation échoue sur des packages dont les dépendances ne sont pas satisfaites, corrigez les packages défectueux, puis exécutez les commandes suivantes.

   `sudo apt --fix-missing update`

   `sudo apt update`

   `sudo apt install -f`

Une fois le téléchargement terminé, vous pouvez vérifier l'authenticité du logiciel téléchargé. Consultez la section Vérifier l'authenticité du logiciel téléchargé à l'étape 1.

Après avoir téléchargé le moniteur Deadline Cloud et vérifié son authenticité, utilisez la procédure suivante pour configurer le moniteur Deadline Cloud.

Pour configurer le moniteur Deadline Cloud

1. Ouvrez le moniteur Deadline Cloud.
2. Lorsque vous êtes invité à créer un nouveau profil, procédez comme suit.
   a. Entrez l'URL de votre moniteur dans l'URL d'entrée, qui ressemble à **`https://`*`MY-MONITOR`*`.deadlinecloud.amazonaws.com/`**
   b. Entrez un nom de profil.
   c. Choisissez Créer un profil.

      Votre profil est créé et vos informations d'identification sont désormais partagées avec tous les logiciels utilisant le nom de profil que vous avez créé.
3. Après avoir créé le profil du moniteur Deadline Cloud, vous ne pouvez pas modifier le nom du profil ni l'URL du studio. Si vous devez apporter des modifications, procédez plutôt comme suit :
   a. Supprimez le profil. Dans le volet de navigation de gauche, choisissez Deadline Cloud monitor, Settings, Delete.
   b. Créez un nouveau profil avec les modifications souhaitées.
4. Dans le volet de navigation de gauche, utilisez l'option >Deadline Cloud monitor pour effectuer les opérations suivantes :
   - Modifiez le profil du moniteur Deadline Cloud pour vous connecter à un autre moniteur.
   - Activez la connexion automatique afin de ne pas avoir à saisir l'URL de votre moniteur lors des prochaines ouvertures du moniteur Deadline Cloud.
5. Fermez la fenêtre de surveillance de Deadline Cloud. Il continue de fonctionner en arrière-plan et de synchroniser vos informations d'identification toutes les 15 minutes.
6. Pour chaque application de création de contenu numérique (DCC) que vous prévoyez d'utiliser pour vos projets de rendu, procédez comme suit :
   a. Depuis votre émetteur Deadline Cloud, ouvrez la configuration du poste de travail Deadline Cloud.

b. Dans la configuration du poste de travail, sélectionnez le profil que vous avez créé dans le moniteur Deadline Cloud. Vos informations d'identification Deadline Cloud sont désormais partagées avec ce DCC et vos outils devraient fonctionner comme prévu.

Étape 3 : Lancez l'émetteur Deadline Cloud

Les sections suivantes vous indiquent les étapes à suivre pour lancer le plugin d'envoi de Deadline Cloud dansBlender, NukeMaya, et. Houdini

Pour lancer l'émetteur Deadline Cloud dans Blender

> **Note**
>
> Support fourni à Blender l'aide de l'Condaenvironnement des flottes gérées par des services. Pour plus d'informations, consultez Environnement de Conda file d'attente par défaut.

1. Ouvrir Blender.
2. Ouvrez une Blender scène dont les dépendances existent dans le répertoire racine de l'actif.
3. Dans le menu Render, sélectionnez la boîte de dialogue Deadline Cloud.
   a. Si vous n'êtes pas encore authentifié dans l'émetteur Deadline Cloud, le statut des informations d'identification indique NEEDS_LOGIN.
   b. Choisissez Login (Connexion).
   c. Une fenêtre de connexion s'affiche dans le navigateur. Connectez-vous à l'aide de vos identifiants d'utilisateur.
   d. Sélectionnez Allow (Autoriser). Vous êtes maintenant connecté et le statut des informations d'identification s'affichera comme AUTHENTIFIÉ.
4. Sélectionnez Envoyer.

Pour lancer l'émetteur Deadline Cloud dans Foundry Nuke

> **Note**
>
> Support fourni à Nuke l'aide de l'Condaenvironnement des flottes gérées par des services. Pour plus d'informations, consultez Environnement de Conda file d'attente par défaut.

1. Ouvrir Nuke.
2. Ouvrez un Nuke script dont les dépendances existent dans le répertoire racine de l'actif.
3. Choisissez Thinkbox, puis Soumettre à Deadline Cloud pour lancer l'expéditeur.
    a. Si vous n'êtes pas déjà authentifié dans l'émetteur Deadline Cloud, le statut des informations d'identification s'affichera sous la forme NEEDS_LOGIN.
    b. Choisissez Login (Connexion).
    c. Dans la fenêtre du navigateur de connexion, connectez-vous à l'aide de vos informations d'identification d'utilisateur.
    d. Sélectionnez Allow (Autoriser). Vous êtes maintenant connecté et le statut des informations d'identification s'affichera comme AUTHENTIFIÉ.
4. Sélectionnez Envoyer.

Pour lancer l'émetteur Deadline Cloud dans Maya

> **Note**
>
> Support pour Maya et Arnold for Maya(MtoA) fourni à l'aide de l'Condaenvironnement pour les flottes gérées par des services. Pour plus d'informations, consultez Environnement de Conda file d'attente par défaut.

1. Ouvrir Maya.
2. Définissez votre projet et ouvrez un fichier qui existe dans le répertoire racine de l'actif.
3. Choisissez Windows → Paramètres/Préférences → Gestionnaire de plugins.
4. Recherchez DeadlineCloudSubmitter.
5. Pour charger le plug-in d'envoi de Deadline Cloud, sélectionnez Loaded.
    a. Si vous n'êtes pas déjà authentifié dans l'émetteur Deadline Cloud, le statut des informations d'identification s'affichera sous la forme NEEDS_LOGIN.
    b. Choisissez Login (Connexion).
    c. Une fenêtre de connexion s'affiche dans le navigateur. Connectez-vous à l'aide de vos identifiants d'utilisateur.
    d. Sélectionnez Allow (Autoriser). Vous êtes maintenant connecté et le statut des informations d'identification s'affiche comme AUTHENTIFIÉ.

6. (Facultatif) Pour charger le plug-in d'envoi de Deadline Cloud à chaque ouvertureMaya, choisissez Chargement automatique.
7. Sélectionnez l'étagère Deadline Cloud, puis cliquez sur le bouton vert pour lancer l'expéditeur.

Pour lancer l'émetteur Deadline Cloud dans Houdini

> **Note**
>
> Support fourni à Houdini l'aide de l'Condaenvironnement des flottes gérées par des services. Pour plus d'informations, consultez Environnement de Conda file d'attente par défaut.

1. Ouvrir Houdini.
2. Dans l'éditeur de réseau, sélectionnez le réseau /out.
3. Appuyez sur la touche Tab et entrez**`deadline`**.
4. Sélectionnez l'option Deadline Cloud et connectez-la à votre réseau existant.
5. Double-cliquez sur le nœud Deadline Cloud.

Pour lancer l'émetteur Deadline Cloud dans KeyShot

Cela suppose que vous avez déjà téléchargé Deadline Cloud et PySide 2.

1. Copiez ou liez le fichier Deadline-Cloud-for-keyshot/keyshot_script/submit à AWS Deadline Cloud.py dans le dossier des scripts. KeyShot

   Par exemple, activéWindows, l'emplacement du dossier des scripts serait**`C:/Users/USER/Documents/KeyShot 12/Scripts`**.
2. Définissez les variables d'environnement suivantes.

   a. Définissez la variable d'environnement **`DEADLINE_PYTHON`** comme chemin d'accès à l'installation Python où se trouvent deadline-cloud et PySide 2.

      Par exemple, onWindows, si vous utilisez Python 3.10, la commande peut être**`set DEADLINE_PYTHON=C:/Users/USER/AppData/Local/Programs/Python/Python310/python`**.

   b. Définissez la variable d'environnement **`DEADLINE_KEYSHOT`** comme chemin d'accès au dossier keyshot_submitter.

Par exemple, onWindows, si la source se trouve sur votre bureau, la commande peut être**`set DEADLINE_KEYSHOT=C:/Users/USER/Desktop/deadline-cloud-for-keyshot/src/deadline/keyshot_submitter`**.

3. Une fois les variables d'environnement définies, lancez KeyShot.
4. Pour lancer l'émetteur depuis KeyShot, choisissez Console de script Windows, Soumettre vers AWS Deadline Cloud et Exécuter.

Pour lancer l'émetteur Deadline Cloud dans Unreal Engine

Cela suppose que vous avez déjà téléchargé Deadline Cloud.

1. Créez ou ouvrez le dossier que vous utilisez pour vos Unreal Engine projets.
2. Ouvrez la ligne de commande et exécutez les commandes suivantes :
   - `git clone https://github.com/aws-deadline/deadline-cloud-for-unreal-engine`
   - `cd deadline-cloud-for-unreal/test_projects`
   - `git lfs fetch –all`
3. Pour télécharger le plugin pourUnreal Engine, ouvrez le dossier Unreal Engine du projet et lancez deadline-cloud-forunreal/test_projects/pull_ue_plugin.bat.

   Cela place les fichiers du plugin dans C :// LocalProjectsUnrealDeadlineCloudTestUnrealDeadlineCloudService/Plugins/.
4. Pour télécharger l'expéditeur, ouvrez le UnrealDeadlineCloudService dossier et lancez-le. **`deadline-cloud-forunreal/ test_projects/Plugins/ UnrealDeadlineCloudService/install_unreal_submitter.bat`**
5. Pour lancer l'émetteur depuisUnreal Engine, procédez comme suit :
   a. Choisissez Edition > Paramètres du projet.
   b. Dans la barre de recherche, saisissez **`movie render pipeline`**.
   c. Réglez les paramètres suivants du pipeline de rendu vidéo :
      i. Pour Default Remote Executor, entrez**`MoviePipelineDeadlineCloudRemote Executor`**.
      ii. Pour Default Executor Job, entrez **`MoviePipelineDeadlineCloudExecutorJob`**

iii. Pour les classes de paramètres de travail par défaut, choisissez le signe plus, puis entrez**`DeadlineCloudRenderStepSetting`**.

Avec ces paramètres, vous pouvez choisir le plugin Deadline Cloud parmiUnreal Engine.

Utilisez la ferme

Si vous avez suivi toutes les instructions de démarrage, vous avez configuré tout ce dont vous avez besoin pour commencer à soumettre des tâches depuis votre poste de travail local à votre ferme, puis à surveiller ces tâches et ressources. Pour plus d'informations sur la soumission de toutes sortes de tâches ou sur le suivi, consultez les rubriques connexes ci-dessous.

- Tâches
- Utilisation du moniteur

Utilisation du moniteur Deadline Cloud

Le moniteur AWS Deadline Cloud vous fournit une vue d'ensemble de vos tâches de calcul visuel. Vous pouvez l'utiliser pour surveiller et gérer les tâches, consulter l'activité des employés sur les flottes, suivre les budgets et l'utilisation, et pour télécharger les résultats d'une tâche.

Chaque file d'attente dispose d'un moniteur de tâches qui vous indique l'état des tâches, des étapes et des tâches. Le moniteur permet de gérer les tâches directement depuis le moniteur. Vous pouvez modifier les priorités, annuler des tâches et les mettre en attente.

Le moniteur Deadline Cloud comporte un tableau qui indique le statut récapitulatif d'une tâche. Vous pouvez également sélectionner une tâche pour consulter les journaux de tâches détaillés qui vous aideront à résoudre les problèmes liés à une tâche.

Vous pouvez utiliser le moniteur Deadline Cloud pour télécharger les résultats à l'emplacement indiqué sur votre poste de travail lors de la création de la tâche.

Le moniteur Deadline Cloud vous aide également à surveiller l'utilisation et à gérer les coûts. Pour plus d'informations, consultez Gestion des budgets et de l'utilisation pour Deadline Cloud.

Rubriques

Partagez l'URL du moniteur Deadline Cloud

Lorsque vous configurez le service Deadline Cloud, vous créez par défaut une URL qui ouvre le moniteur Deadline Cloud pour votre compte. Utilisez cette URL pour ouvrir le moniteur dans votre

navigateur ou sur votre bureau. Partagez l'URL avec d'autres utilisateurs afin qu'ils puissent accéder au moniteur Deadline Cloud.

Avant qu'un utilisateur puisse ouvrir le moniteur Deadline Cloud, vous devez lui accorder l'accès. Pour accorder l'accès, ajoutez l'utilisateur à la liste des utilisateurs autorisés pour le moniteur ou ajoutez-le à un groupe ayant accès au moniteur. Pour plus d'informations, consultez Gestion des utilisateurs dans Deadline Cloud.

Pour partager l'URL du moniteur

1. Ouvrez la console Deadline Cloud.
2. Dans Commencer, choisissez Accéder au tableau de bord de Deadline Cloud.
3. Dans le volet de navigation, sélectionnez Dashboard (Tableau de bord).
4. Dans la section Aperçu du compte, sélectionnez Détails du compte.
5. Copiez puis envoyez en toute sécurité l'URL à toute personne ayant besoin d'accéder au moniteur Deadline Cloud.

Ouvrez le moniteur Deadline Cloud

Vous pouvez ouvrir le moniteur Deadline Cloud de l'une des manières suivantes :

- Console : connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la.
- Web : accédez à l'URL du moniteur que vous avez créée lors de la configuration de Deadline Cloud.
- Surveiller — Utilisez le moniteur Deadline Cloud pour ordinateur de bureau.

Lorsque vous utilisez la console, vous devez être en mesure de vous connecter à AWS l'aide d'une AWS Identity and Access Management identité, puis de vous connecter au moniteur avec des AWS IAM Identity Center informations d'identification. Si vous ne disposez que des informations d'identification IAM Identity Center, vous devez vous connecter à l'aide de l'URL du moniteur ou de l'application de bureau.

Pour ouvrir le moniteur Deadline Cloud (web)

1. À l'aide d'un navigateur, ouvrez l'URL du moniteur que vous avez créée lors de la configuration de Deadline Cloud.
2. Connectez-vous à l'aide de vos informations d'identification d'utilisateur.

Pour ouvrir le moniteur Deadline Cloud (console)

1. Ouvrez la console Deadline Cloud.
2. Dans le volet de navigation, sélectionnez Fermes.
3. Sélectionnez une ferme, puis choisissez Gérer les tâches pour ouvrir la page de surveillance de Deadline Cloud.
4. Connectez-vous à l'aide de vos informations d'identification d'utilisateur.

Pour ouvrir le moniteur Deadline Cloud (ordinateur de bureau)

1. Ouvrez la console Deadline Cloud.

   -ou-

   Ouvrez le moniteur Deadline Cloud - Web à partir de l'URL du moniteur.
2. - Sur la console Deadline Cloud, procédez comme suit :
     1. Sur le moniteur, choisissez Accéder au tableau de bord de Deadline Cloud, puis sélectionnez Téléchargements dans le menu de gauche.
     2. Dans le moniteur Deadline Cloud, choisissez la version du moniteur pour votre ordinateur de bureau.
     3. Choisissez Téléchargement.
   - Sur le moniteur Web de Deadline Cloud, procédez comme suit :
     - Dans le menu de gauche, choisissez Configuration du poste de travail. Si l'élément de configuration du poste de travail n'est pas visible, utilisez la flèche pour ouvrir le menu de gauche.
     - Choisissez Téléchargement.
     - Dans Sélectionnez un système d'exploitation, sélectionnez votre système d'exploitation.
3. Téléchargez le moniteur Deadline Cloud pour ordinateur.
4. Après avoir téléchargé et installé le moniteur, ouvrez-le sur votre ordinateur.

   - Si c'est la première fois que vous ouvrez le moniteur Deadline Cloud, vous devez fournir l'URL du moniteur et créer un nom de profil. Ensuite, vous vous connectez au moniteur avec vos informations d'identification Deadline Cloud.
   - Après avoir créé un profil, vous pouvez ouvrir le moniteur en sélectionnant un profil. Vous devrez peut-être saisir vos informations d'identification Deadline Cloud.

Afficher les détails de la file d'attente et de la flotte dans Deadline Cloud

Vous pouvez utiliser le moniteur Deadline Cloud pour visualiser la configuration des files d'attente et des flottes de votre ferme. Vous pouvez également utiliser le moniteur pour voir la liste des tâches d'une file d'attente ou des travailleurs d'un parc de véhicules.

Vous devez être `VIEWING` autorisé à consulter les détails de la file d'attente et de la flotte. Si les informations ne s'affichent pas, contactez votre administrateur pour obtenir les autorisations appropriées.

Pour afficher les détails de la file d'attente

1. Ouvrez le moniteur Deadline Cloud.
2. Dans la liste des fermes, choisissez la ferme qui contient la file d'attente qui vous intéresse.
3. Dans la liste des files d'attente, choisissez une file pour afficher ses détails. Pour comparer la configuration de deux files d'attente ou plus, cochez plusieurs cases.
4. Pour voir la liste des tâches de la file d'attente, choisissez le nom de la file d'attente dans la liste des files d'attente ou dans le panneau de détails.

Si le moniteur est déjà ouvert, vous pouvez sélectionner la file d'attente dans la liste des files d'attente du volet de navigation de gauche.

Pour afficher les détails d'une flotte

1. Ouvrez le moniteur Deadline Cloud.
2. Dans la liste des fermes, choisissez la ferme qui contient la flotte qui vous intéresse.
3. Dans Ressources agricoles, sélectionnez Fleets.
4. Dans la liste des flottes, choisissez une flotte pour en afficher les détails. Pour comparer la configuration de deux flottes ou plus, cochez plusieurs cases.
5. Pour voir la liste des travailleurs de la flotte, choisissez le nom de la flotte dans la liste des flottes ou dans le panneau des détails.

Si le moniteur est déjà ouvert, vous pouvez sélectionner la flotte dans la liste des flottes du volet de navigation de gauche.

Afficher et gérer les tâches, les étapes et les tâches dans Deadline Cloud

Lorsque vous sélectionnez une file d'attente, la section de surveillance des tâches du moniteur Deadline Cloud affiche les tâches de cette file d'attente, les étapes de la tâche et les tâches de chaque étape. Lorsque vous sélectionnez une tâche, une étape ou une tâche, vous pouvez utiliser le menu Actions pour les gérer.

Pour ouvrir le moniteur de tâches, suivez les étapes pour afficher une file d'attenteAfficher les détails de la file d'attente et de la flotte dans Deadline Cloud, puis sélectionnez le travail, l'étape ou la tâche à utiliser.

Pour les tâches, les étapes et les tâches, vous pouvez effectuer les opérations suivantes :

- Modifiez le statut sur En attente, Succès, Échec ou Annulé.
- Téléchargez le résultat traité à partir de la tâche, de l'étape ou de la tâche.
- Copiez l'ID de la tâche, de l'étape ou de la tâche.

Pour la tâche sélectionnée, vous pouvez :

- Archivez le job.
- Modifiez les propriétés de la tâche, par exemple en modifiant la priorisation ou en visualisant les interdépendances étape par étape.
- Affichez des détails supplémentaires à l'aide des paramètres de la tâche.

Pour plus d'informations, consultez Afficher les détails du poste dans Deadline Cloud.

Pour chaque étape, vous pouvez :

- Affichez les dépendances de l'étape. Les dépendances d'une étape doivent être terminées avant que l'étape ne s'exécute.

Pour plus de détails, consultez Afficher une étape dans Deadline Cloud.

Pour chaque tâche, vous pouvez :

- Afficher les journaux de la tâche.

- Afficher les paramètres des tâches.

Pour plus d'informations, consultez Afficher une tâche dans Deadline Cloud.

Afficher les détails du poste dans Deadline Cloud

La page Job monitor de Deadline Cloud Monitor fournit les informations suivantes :

- Vue d'ensemble de l'avancement d'une tâche.
- Vue des étapes et des tâches qui constituent le travail.

Choisissez une tâche dans la liste pour afficher la liste des étapes de la tâche, puis choisissez une étape dans la liste des étapes pour afficher les tâches associées à la tâche. Après avoir choisi un élément, vous pouvez utiliser le menu Actions correspondant à cet élément pour en afficher les détails.

Pour consulter les détails du poste

1. Suivez les étapes pour afficher une file d'attente dansAfficher les détails de la file d'attente et de la flotte dans Deadline Cloud.
2. Dans le volet de navigation, sélectionnez la file d'attente dans laquelle vous avez soumis votre tâche.
3. Sélectionnez une tâche à l'aide de l'une des méthodes suivantes :

    a. Dans la liste des tâches, sélectionnez une tâche pour en afficher les détails.

    b. Dans le champ de recherche, entrez le texte associé à la tâche, tel que le nom de la tâche ou l'utilisateur qui l'a créée. Dans les résultats qui s'affichent, sélectionnez le travail que vous souhaitez consulter.

Les détails d'une tâche incluent les étapes de la tâche et les tâches de chaque étape. Vous pouvez utiliser le menu Actions pour effectuer les opérations suivantes :

- Modifiez le statut de la tâche.
- Affichez et modifiez les propriétés d'une tâche. Vous pouvez afficher les dépendances entre les étapes de la tâche et modifier la priorité de la tâche. En général, les tâches ayant une priorité plus élevée sont terminées plus tôt.

- Affichez les paramètres de la tâche qui ont été définis lors de son envoi.
- Téléchargez le résultat d'une tâche. Lorsque vous téléchargez le résultat d'un travail, celui-ci contient tous les résultats générés par les étapes et les tâches du travail.

Afficher une étape dans Deadline Cloud

Utilisez le moniteur AWS Deadline Cloud pour visualiser les étapes de vos tâches de traitement. Dans le moniteur de tâches, la liste des étapes affiche la liste des étapes composant le travail sélectionné. Lorsque vous sélectionnez une étape, la liste des tâches affiche les tâches de l'étape.

Pour consulter une étape

1. Suivez les étapes ci-dessous Afficher les détails du poste dans Deadline Cloud pour afficher la liste des offres d'emploi.
2. Sélectionnez une tâche dans la liste de Tâches.
3. Sélectionnez une étape dans la liste des étapes.

Vous pouvez utiliser le menu Actions pour effectuer les opérations suivantes :

- Modifiez le statut de l'étape.
- Téléchargez le résultat de l'étape. Lorsque vous téléchargez le résultat d'une étape, celui-ci contient tous les résultats générés par les tâches de l'étape.
- Affichez les dépendances d'une étape. Le tableau des dépendances présente une liste des étapes qui doivent être terminées avant que l'étape sélectionnée ne commence, ainsi qu'une liste des étapes en attente de la fin de cette étape.

Afficher une tâche dans Deadline Cloud

Utilisez le moniteur AWS Deadline Cloud pour visualiser les tâches de vos tâches de traitement. Dans le Moniteur des tâches, la liste des tâches affiche les tâches qui constituent l'étape sélectionnée dans la liste des étapes.

Pour afficher une tâche

1. Suivez les étapes ci-dessous Afficher les détails du poste dans Deadline Cloud pour afficher la liste des offres d'emploi.

2. Sélectionnez une tâche dans la liste de Tâches.
3. Sélectionnez une étape dans la liste des étapes.
4. Sélectionnez une tâche dans la liste des tâches.

Vous pouvez utiliser le menu Actions pour effectuer les opérations suivantes :

- Modifiez le statut de la tâche.
- Afficher les journaux des tâches. Pour plus d'informations, consultez Afficher les journaux dans Deadline Cloud.
- Affichez les paramètres définis lors de la création de la tâche.
- Téléchargez le résultat de la tâche. Lorsque vous téléchargez le résultat d'une tâche, celui-ci contient uniquement le résultat généré par la tâche sélectionnée.

Afficher les journaux dans Deadline Cloud

Les journaux vous fournissent des informations détaillées sur le statut et le traitement des tâches. Dans le moniteur AWS Deadline Cloud, vous pouvez voir les deux types de journaux suivants :

- Les journaux de session détaillent le calendrier des actions, notamment :
  - Actions de configuration, telles que la synchronisation des pièces jointes et le chargement de l'environnement logiciel
  - Exécution d'une tâche ou d'un ensemble de tâches
  - Actions de fermeture, telles que la fermeture de l'environnement d'un travailleur

  Une session inclut le traitement d'au moins une tâche et peut inclure plusieurs tâches. Les journaux de session contiennent également des informations sur le type d'instance Amazon Elastic Compute Cloud (Amazon EC2), le vCPU et la mémoire. Les journaux de session incluent également un lien vers le journal du travailleur utilisé dans la session.
- Les journaux des travailleurs fournissent des détails sur la chronologie des actions qu'un travailleur exécute au cours de son cycle de vie. Les journaux des travailleurs peuvent contenir des informations sur plusieurs sessions.

Vous pouvez télécharger les journaux de session et de travail afin de pouvoir les consulter hors ligne.

Pour consulter les journaux de session

1. Suivez les étapes ci-dessous Afficher les détails du poste dans Deadline Cloud pour afficher la liste des offres d'emploi.
2. Sélectionnez une tâche dans la liste de Tâches.
3. Sélectionnez une étape dans la liste des étapes.
4. Sélectionnez une tâche dans la liste des tâches.
5. Dans le menu Actions, choisissez Afficher les journaux.

La section Chronologies présente un résumé des actions associées à la tâche. Pour voir d'autres tâches exécutées au cours de la session et pour voir les actions de fermeture de la session, choisissez Afficher les journaux de toutes les tâches.

Pour consulter les journaux des employés à partir d'une tâche

1. Suivez les étapes ci-dessous Afficher les détails du poste dans Deadline Cloud pour afficher la liste des offres d'emploi.
2. Sélectionnez une tâche dans la liste de Tâches.
3. Sélectionnez une étape dans la liste des étapes.
4. Sélectionnez une tâche dans la liste des tâches.
5. Dans le menu Actions, choisissez Afficher les journaux.
6. Choisissez Informations sur la session.
7. Choisissez Afficher le journal des travailleurs.

Pour consulter les journaux des travailleurs à partir des détails du parc

1. Suivez les étapes ci-dessous Afficher les détails de la file d'attente et de la flotte dans Deadline Cloud pour voir une flotte.
2. Sélectionnez un ID de travailleur dans la liste des travailleurs.
3. Dans le menu Actions, choisissez Afficher les journaux des travailleurs.

Télécharger le résultat final dans Deadline Cloud

Une fois le travail terminé, vous pouvez utiliser le moniteur AWS Deadline Cloud pour télécharger les résultats sur votre poste de travail. Le fichier de sortie est stocké avec le nom et l'emplacement que vous avez spécifiés lors de la création de la tâche.

Les fichiers de sortie sont stockés indéfiniment. Pour réduire les coûts de stockage, pensez à créer une configuration S3 Lifecycle pour le compartiment Amazon S3 de votre file d'attente. Pour plus d'informations, consultez Gérer votre cycle de vie de stockage dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour télécharger le résultat final d'une tâche, d'une étape ou d'une tâche

1. Suivez les étapes ci-dessous Afficher les détails du poste dans Deadline Cloud pour afficher la liste des offres d'emploi.
2. Sélectionnez le travail, l'étape ou la tâche pour laquelle vous souhaitez télécharger le résultat.
   - Si vous sélectionnez une tâche, vous pouvez télécharger tous les résultats correspondant à toutes les tâches correspondant à toutes les étapes de cette tâche.
   - Si vous sélectionnez une étape, vous pouvez télécharger tous les résultats pour toutes les tâches de cette étape.
   - Si vous sélectionnez une tâche, vous pouvez télécharger le résultat correspondant à cette tâche individuelle.
3. Dans le menu Actions, choisissez Télécharger le résultat.
4. La sortie sera téléchargée à l'emplacement défini lors de la soumission de la tâche.

> **Note**
>
> Le téléchargement de la sortie à l'aide du menu n'est actuellement pris en charge que pour Windows etLinux. Si vous avez un Mac et que vous choisissez l'élément de menu Télécharger la sortie, une fenêtre affiche la AWS CLI commande que vous pouvez utiliser pour télécharger la sortie rendue.

Fermes cloud Deadline

Un parc est un conteneur pour les files d'attente qui gèrent les tâches et les flottes de ressources informatiques qui exécutent des tâches.

Rubriques

Création d'une ferme

1. Dans la console Deadline Cloud, choisissez Accéder au tableau de bord.
2. Dans la section Fermes du tableau de bord de Deadline Cloud, choisissez Actions → Créer une ferme.

   - Sinon, dans le panneau de gauche, choisissez Fermes et autres ressources, puis choisissez Créer une ferme.
3. Ajoutez un nom à votre ferme.
4. Dans Description, entrez la description de la ferme. Une description claire peut vous aider à identifier rapidement l'objectif de votre exploitation.
5. (Facultatif) Par défaut, vos données sont cryptées à l'aide d'une clé qui AWS détient et gère votre sécurité. Vous pouvez choisir Personnaliser les paramètres de chiffrement (avancés) pour utiliser une clé existante ou pour en créer une nouvelle que vous gérez.

   Si vous choisissez de personnaliser les paramètres de chiffrement à l'aide de la case à cocher, entrez un AWS KMS ARN ou créez-en un nouveau AWS KMS en choisissant Créer une nouvelle clé KMS.
6. (Facultatif) Choisissez Ajouter un nouveau tag pour ajouter un ou plusieurs tags à votre ferme.
7. Choisissez Create farm. Une fois créée, votre ferme s'affiche.

Supprimer une ferme

1. Dans le tableau de bord de Deadline Cloud, sélectionnez Fermes et autres ressources.

2. Dans la liste des fermes, sélectionnez la ou les fermes que vous souhaitez supprimer, puis choisissez Supprimer.

Modifier une ferme

1. Dans le tableau de bord de Deadline Cloud, sélectionnez Fermes et autres ressources.
2. Dans la liste des fermes, sélectionnez la ou les fermes que vous souhaitez supprimer, puis choisissez Modifier.
3. Dans la fenêtre d'édition qui s'affiche, modifiez le nom ou la description de la ferme, puis choisissez Enregistrer les modifications.

Files d'attente de Deadline Cloud

Une file d'attente est une ressource agricole qui gère et traite les tâches.

Pour travailler avec des files d'attente, vous devez déjà avoir configuré un moniteur et une ferme.

Rubriques

Créer une file d'attente

1. Dans le tableau de bord de la console Deadline Cloud, sélectionnez le parc pour lequel vous souhaitez créer une file d'attente.

    - Sinon, dans le panneau de gauche, choisissez Fermes et autres ressources, puis sélectionnez la ferme pour laquelle vous souhaitez créer une file d'attente.
2. Dans l'onglet Files d'attente, choisissez Créer une file d'attente.
3. Entrez un nom pour votre file d'attente.
4. Dans Description, entrez la description de la file d'attente. Une description vous aide à identifier l'objectif de votre file d'attente.
5. Pour les pièces jointes aux Job, vous pouvez soit créer un nouveau compartiment Amazon S3, soit choisir un compartiment Amazon S3 existant.

    a. Pour créer un nouveau compartiment Amazon S3

        i. Sélectionnez Créer un nouveau compartiment de tâches.

        ii. Entrez un nom pour le compartiment. Nous vous recommandons de donner un nom au bucket`deadlinecloud-job-attachments-[MONITORNAME]`.

        iii. Entrez un préfixe racine pour définir ou modifier l'emplacement racine de votre file d'attente.

    b. Pour choisir un compartiment Amazon S3 existant

i. Sélectionnez Choisir un compartiment S3 existant > Parcourir S3.

ii. Sélectionnez le compartiment S3 pour votre file d'attente dans la liste des compartiments disponibles.

6. (Facultatif) Pour associer votre file d'attente à un parc géré par le client, sélectionnez Activer l'association aux flottes gérées par le client.

7. Si vous activez l'association avec des flottes gérées par le client, vous devez suivre les étapes suivantes.

> **Important**
>
> Nous vous recommandons vivement de spécifier des utilisateurs et des groupes pour la fonctionnalité d'exécution en tant que telle. Si vous ne le faites pas, cela dégradera le niveau de sécurité de votre exploitation, car les tâches peuvent alors faire tout ce que l'agent du travailleur peut faire. Pour plus d'informations sur les risques de sécurité potentiels, voir Exécuter des tâches en tant qu'utilisateurs et en tant que groupes.

a. Pour Exécuter en tant qu'utilisateur :

Pour fournir des informations d'identification pour les tâches de la file d'attente, sélectionnez Utilisateur configuré dans la file d'attente.

Ou, pour refuser de définir vos propres informations d'identification et d'exécuter des tâches en tant qu'utilisateur de l'agent de travail, sélectionnez l'utilisateur de l'agent de travail.

b. (Facultatif) Pour Exécuter en tant qu'informations d'identification utilisateur, entrez un nom d'utilisateur et un nom de groupe pour fournir des informations d'identification pour les tâches de la file d'attente.

Si vous utilisez une Windows flotte, vous devez créer un AWS Secrets Manager secret contenant le mot de passe pour exécuter en tant qu'utilisateur. Suivez ces instructions pour créer le secret. Remplacez *jobuser* par le nom du`jobRunAsUser`.

i. Ouvrez PowerShell ou lancez une invite de commande en tant qu'administrateur.

ii. Créez l'utilisateur.

```
net user jobuser /add
```

iii. Définissez le mot de passe.

```
net user jobuser *
```

iv. Créez un profil local et un répertoire personnel pour l'utilisateur. Exécutez la commande suivante et entrez le mot de passe de l'utilisateur lorsque vous y êtes invité.

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

8. Le fait d'exiger un budget permet de gérer les coûts de votre file d'attente. Sélectionnez Ne pas exiger de budget ou Exiger un budget.
9. Votre file d'attente nécessite une autorisation pour accéder à Amazon S3 en votre nom. Vous pouvez créer un nouveau rôle de service ou utiliser un rôle de service existant. Si vous n'avez pas de rôle de service existant, créez-en un nouveau et utilisez-en un nouveau.

   a. Pour utiliser un rôle de service existant, sélectionnez Choisir un rôle de service, puis sélectionnez un rôle dans la liste déroulante.

   b. Pour créer un nouveau rôle de service, sélectionnez Créer et utiliser un nouveau rôle de service, puis entrez un nom et une description du rôle.

10. (Facultatif) Pour ajouter des variables d'environnement pour l'environnement de file d'attente, choisissez Ajouter une nouvelle variable d'environnement, puis entrez un nom et une valeur pour chaque variable que vous ajoutez.
11. (Facultatif) Choisissez Ajouter un nouveau tag pour ajouter un ou plusieurs tags à votre file d'attente.
12. Pour créer un environnement de Conda file d'attente par défaut, maintenez la case à cocher sélectionnée. Pour en savoir plus sur les environnements de file d'attente, voir Création d'un environnement de file d'attente. Si vous créez une file d'attente pour un parc géré par le client, décochez la case.
13. Choisissez Créez une file d'attente.

Création d'un environnement de file d'attente

Un environnement de file d'attente est un ensemble de variables et de commandes d'environnement qui configurent les employés du parc automobile. Vous pouvez utiliser les environnements de

file d'attente pour fournir des applications logicielles, des variables d'environnement et d'autres ressources aux tâches de la file d'attente.

Lorsque vous créez une file d'attente, vous avez la possibilité de créer un environnement de Conda file d'attente par défaut. Cet environnement permet aux flottes gérées par les services d'accéder aux packages destinés aux applications et moteurs de rendu DCC partenaires. Pour plus d'informations, consultez Environnement de Conda file d'attente par défaut.

Vous pouvez ajouter des environnements de file d'attente à l'aide de la console ou en modifiant directement le modèle json ou YAML. Cette procédure décrit comment créer un environnement avec la console.

1. Pour ajouter un environnement de file d'attente à une file d'attente, accédez à la file d'attente et sélectionnez l'onglet Environnements de file d'attente.
2. Choisissez Actions, puis Créer un nouveau formulaire.
3. Entrez un nom et une description pour l'environnement de file d'attente.
4. Choisissez Ajouter une nouvelle variable d'environnement, puis entrez un nom et une valeur pour chaque variable que vous ajoutez.
5. (Facultatif) Entrez une priorité pour l'environnement de file d'attente. La priorité indique l'ordre dans lequel cet environnement de file d'attente sera exécuté sur le travailleur. Les environnements de file d'attente ayant une priorité plus élevée seront exécutés en premier.
6. Choisissez Créer un environnement de file d'attente.

Environnement de Conda file d'attente par défaut

Lorsque vous créez une file d'attente associée à un parc géré par des services, vous avez la possibilité d'ajouter un environnement de file d'attente par défaut qui prend en charge Condale téléchargement et l'installation de packages dans un environnement virtuel pour vos tâches.

Condafournit des forfaits à partir de chaînes. Un canal est un emplacement où les packages sont stockés. Deadline Cloud fournit un canal qui héberge des packages compatibles avec les applications et les moteurs de rendu DCC partenaires. `deadline-cloud` Les packages sont les suivants :

- Mixeur
  - `blender=3.6`

  - `blender-openjd`
- Houdini
  - `houdini=19.5`
  - `houdini-openjd`
- Maya
  - `maya=2024`
  - `maya-mtoa=2024.5.3`
  - `maya-openjd`
- Nuke
  - `nuke=15`
  - `nuke-openjd`

Lorsque vous soumettez une tâche à une file d'attente avec l'Condaenvironnement par défaut, l'environnement ajoute deux paramètres à la tâche. Ces paramètres spécifient les Conda packages et les canaux à utiliser pour configurer l'environnement de la tâche avant le traitement des tâches. Les paramètres sont les suivants :

- `CondaPackages`— une liste séparée par des espaces des spécifications de correspondance des packages, telles `blender=3.6` que ou. `numpy>1.22` La valeur par défaut est vide pour ignorer la création d'un environnement virtuel.
- `CondaChannels`— une liste de Condachaînes séparées par des espaces, par exemple `deadline-cloudconda-forge`, ou`s3://DOC-EXAMPLE-BUCKET/conda/channel`. Par défaut`deadline-cloud`, il s'agit d'un canal accessible aux flottes gérées par des services qui fournit des applications et des moteurs de rendu DCC partenaires.

Lorsque vous utilisez un émetteur intégré pour envoyer une tâche à Deadline Cloud depuis votre DCC, l'émetteur renseigne la valeur du `CondaPackages` paramètre en fonction de l'application DCC et de l'expéditeur. Par exemple, si vous utilisez Blender, le `CondaPackage` paramètre est défini sur`blender=3.6.* blender-openjd=0.4.*`.

Suppression d'une file d'attente

> **Warning**
>
> Vous ne pouvez pas récupérer les tâches d'une file d'attente si vous supprimez cette dernière. La suppression de la file d'attente entraîne également la suppression des tâches qu'elle contient.

1. Dans le tableau de bord de Deadline Cloud, sélectionnez Fermes et autres ressources.
2. Dans la liste des parcs de serveurs, sélectionnez le parc contenant la file d'attente à supprimer.
3. Sélectionnez la file d'attente, puis choisissez Supprimer.
4. Dans la fenêtre de confirmation, choisissez Delete. Votre file d'attente et toutes les tâches qu'elle contient sont supprimées.

Modifier une file d'attente

1. Dans le tableau de bord de Deadline Cloud, sélectionnez Fermes et autres ressources.
2. Dans la liste des fermes, sélectionnez la batterie contenant la file d'attente à modifier.
3. Sélectionnez la file d'attente, puis choisissez Modifier.
4. Vous pouvez modifier le nom, la description, le budget requis, l'option Exécuter en tant qu'utilisateur et le rôle de service attribué. Vous pouvez également associer une flotte existante à votre file d'attente.
5. Sélectionnez Enregistrer les modifications.

Associer une file d'attente et une flotte

1. Sélectionnez la file d'attente que vous souhaitez associer à une flotte.
2. Pour sélectionner une flotte à associer à votre file d'attente, choisissez Associer des flottes.
3. Choisissez le menu déroulant Sélectionner des flottes. La liste des flottes disponibles s'affiche.
4. Dans la liste des flottes disponibles, cochez la case à côté de la flotte ou des flottes que vous souhaitez associer à votre file d'attente.
5. Choisissez Associer. Le statut d'association de flotte doit désormais être Associé.

Gérer les flottes de Deadline Cloud

Cette section explique comment gérer les flottes gérées par les services (SMF) et les flottes gérées par le client (CMF) pour Deadline Cloud.

Vous pouvez configurer deux types de flottes Deadline Cloud :

- Les flottes gérées par des services sont des flottes de travailleurs dont les paramètres par défaut sont fournis par ce service, Deadline Cloud. Ces paramètres par défaut sont conçus pour être efficaces et économiques.
- Les flottes gérées par le client (CMF) sont des flottes de travailleurs que vous gérez. Un CMF peut résider dans une AWS infrastructure, sur site ou dans un centre de données colocalisé. Un CMF assure le contrôle total et la responsabilité de la flotte. Cela inclut le provisionnement, les opérations, la gestion et le démantèlement du personnel de la flotte.

Rubriques

Gérez les flottes gérées par le service Deadline Cloud

Les flottes gérées par des services sont des flottes de travailleurs dont les paramètres par défaut sont fournis par Deadline Cloud. Ces paramètres par défaut sont conçus pour être efficaces et économiques.

1. Pour créer une flotte gérée par des services (SMF), accédez à la ferme dans laquelle vous souhaitez créer la flotte.
2. Sélectionnez l'onglet Flottes.
3. Choisissez Create fleet (Créer une flotte).
4. Entrez le nom de votre flotte.
5. Saisissez une Description. Une description claire peut vous aider à identifier rapidement l'objectif de votre flotte.
6. Sélectionnez le type de flotte géré par le service.

7. Choisissez l'option de marché des instances ponctuelles ou à la demande pour votre flotte. Les instances ponctuelles sont des capacités non réservées que vous pouvez utiliser à un prix réduit, mais qui peuvent être interrompues par des demandes à la demande. Les instances à la demande sont facturées à la seconde, mais n'ont aucun engagement à long terme et ne seront pas interrompues. Par défaut, les flottes utilisent des instances Spot.
8. Facultatif Définissez le nombre maximum d'instances pour dimensionner le parc afin que la capacité soit disponible pour les tâches de la file d'attente. Nous vous recommandons de maintenir le nombre minimum d'instances à ce niveau **0** afin de garantir que le parc libère toutes les instances lorsqu'aucune tâche n'est mise en file d'attente.
9. Pour accéder aux services de votre flotte, sélectionnez un rôle existant ou créez-en un nouveau. Un rôle de service fournit des informations d'identification aux instances du parc, leur accordant l'autorisation de traiter les tâches, et aux utilisateurs du moniteur, afin qu'ils puissent lire les informations du journal.
10. Choisissez Suivant.
11. Entrez les processeurs virtuels minimum et maximum dont vous avez besoin pour votre parc.
12. Entrez la mémoire minimale et maximale dont vous avez besoin pour votre flotte.
13. Facultatif Vous pouvez choisir d'autoriser ou d'exclure des types d'instances spécifiques de votre parc afin de garantir que seuls ces types d'instances sont utilisés pour ce parc.
14. Facultatif Vous pouvez spécifier la taille du volume Amazon Elastic Block Store (Amazon EBS) gp3 qui sera attaché aux travailleurs de ce parc. Pour plus d'informations, consultez le guide de l'utilisateur d'EBS.
15. Choisissez Suivant.
16. Facultatif Définissez des exigences personnalisées en matière de personnel qui définissent les caractéristiques de ce parc qui peuvent être combinées avec les exigences d'hôte personnalisées spécifiées dans les soumissions de tâches. Par exemple, un type de licence particulier est celui d'un type de licence si vous prévoyez de connecter votre flotte à votre propre serveur de licences.
17. Choisissez Suivant.
18. Facultatif Pour associer votre flotte à une file d'attente, sélectionnez une file d'attente dans le menu déroulant. Si la file d'attente est configurée avec l'environnement de Conda file d'attente par défaut, votre flotte reçoit automatiquement des packages compatibles avec les applications et les moteurs de rendu DCC partenaires. Pour obtenir la liste des packages fournis, consultezEnvironnement de Conda file d'attente par défaut.
19. Choisissez Suivant.

20. Facultatif Pour ajouter une étiquette à votre flotte, choisissez Ajouter une nouvelle étiquette, puis entrez la clé et la valeur de cette étiquette.
21. Choisissez Suivant.
22. Passez en revue les paramètres de votre flotte, puis choisissez Créer une flotte. Après sa création, votre flotte s'affiche.

Compatibilité VFX Reference Platform

VFX Reference PlatformIl s'agit d'une plate-forme cible courante pour l'industrie des effets visuels. Pour utiliser l'instance Amazon EC2 de parc géré par des services standard exécutant Amazon Linux 2023 avec un logiciel compatible, vous devez tenir compte VFX Reference Platform des considérations suivantes lorsque vous utilisez un parc géré par des services.

VFX Reference PlatformIl est mis à jour chaque année. Ces considérations relatives à l'utilisation d'un AL2023, y compris les flottes gérées par le service Deadline Cloud, sont basées sur les plateformes de référence de l'année civile (CY) 2022 à 2024. Pour plus d'informations, consultez VFX Reference Platform.

> **Note**
>
> Si vous créez un custom Amazon Machine Image (AMI) pour un parc géré par le client, vous pouvez ajouter ces exigences lorsque vous préparez l'instance Amazon EC2.

Pour utiliser un logiciel VFX Reference Platform pris en charge sur une instance Amazon EC2 AL2023, tenez compte des points suivants :

- La version glibc installée avec AL2023 est compatible pour une utilisation en environnement d'exécution, mais pas pour la création de logiciels compatibles avec le VFX Reference Platform CY2024 ou une version antérieure.
- Python 3.9 et 3.11 sont fournis avec le parc géré par les services, ce qui le rend compatible avec VFX Reference Platform CY2022 et CY2024. Python 3.7 et 3.10 ne sont pas fournis dans le parc géré par les services. Les logiciels qui les nécessitent doivent fournir l'installation de Python dans la file d'attente ou dans l'environnement de travail.
- Certains composants de la bibliothèque Boost fournis dans le parc géré par les services sont en version 1.75, qui n'est pas compatible avec le. VFX Reference Platform Si votre application utilise Boost, vous devez fournir votre propre version de la bibliothèque pour des raisons de compatibilité.

- La mise à jour 3 d'Intel TBB est fournie dans le parc géré par les services. Ceci est compatible avec VFX Reference Platform CY2022, CY2023 et CY2024.
- Les autres bibliothèques dont les versions sont spécifiées par le ne VFX Reference Platform sont pas fournies par le parc géré par le service. Vous devez fournir à la bibliothèque toute application utilisée sur un parc géré par des services. Pour une liste des bibliothèques, consultez la plateforme de référence.

Gérez les flottes gérées par les clients de Deadline Cloud

Cette section explique comment gérer une flotte gérée par le client (CMF) pour Deadline Cloud.

Les CMF sont des flottes de travailleurs que vous gérez. Un CMF peut résider dans une AWS infrastructure, sur site ou dans un centre de données colocalisé. Un CMF assure le contrôle total et la responsabilité de la flotte. Cela inclut le provisionnement, les opérations, la gestion et le démantèlement du personnel de la flotte.

Rubriques

Créez une flotte gérée par le client

Pour créer une flotte gérée par le client (CMF), procédez comme suit.

Deadline Cloud console

Pour utiliser la console Deadline Cloud pour créer une flotte gérée par le client

1. Ouvrez la console Deadline Cloud.

2. Sélectionnez Fermes. La liste des fermes disponibles s'affiche.
3. Sélectionnez le nom de la ferme dans laquelle vous souhaitez travailler.
4. Sélectionnez l'onglet Flottes.
5. Choisissez Create fleet (Créer une flotte).
6. Entrez le nom de votre flotte.
7. (Facultatif) Entrez une description pour votre flotte.
8. Sélectionnez Géré par le client pour le type de flotte.
9. Sélectionnez un type d'Auto Scaling. Pour plus d'informations, consultez Utiliser EventBridge pour gérer les événements Auto Scaling.

   - Aucune mise à l'échelle : vous créez une flotte sur site et souhaitez vous désinscrire de Deadline Cloud Auto Scaling.
   - Recommandations de dimensionnement : vous êtes en train de créer une flotte Amazon Elastic Compute Cloud (Amazon EC2).
10. Sélectionnez l'accès aux services de votre flotte.

    a. Nous vous recommandons d'utiliser l'option Créer et utiliser un nouveau rôle de service pour chaque flotte pour un contrôle des autorisations plus précis. Cette option est sélectionnée par défaut.

    b. Vous pouvez également utiliser un rôle de service existant en sélectionnant Choisir un rôle de service.
11. Passez en revue vos sélections, puis choisissez Next.
12. Sélectionnez un système d'exploitation pour votre flotte. Tous les employés d'une flotte doivent disposer d'un système d'exploitation commun.
13. Sélectionnez l'architecture du processeur hôte.
14. Sélectionnez la configuration matérielle requise suivante pour les hôtes subordonnés de ce parc.

    a. Sélectionnez les exigences minimales et maximales en termes de vCPU et de mémoire pour répondre aux exigences de charge de travail de vos flottes.

    b. (Facultatif) Sélectionnez la configuration graphique requise, puis entrez les GPU minimum et maximum.
15. Passez en revue vos sélections, puis choisissez Next.
16. (Facultatif) Définissez des exigences personnalisées pour les travailleurs.

17. À l'aide de la liste déroulante, sélectionnez une ou plusieurs files d'attente à associer à la flotte.

> **Note**
>
> Nous recommandons d'associer une flotte uniquement aux files d'attente situées toutes dans la même limite de confiance. Cela garantit une limite de sécurité solide entre les tâches exécutées par le même travailleur.

18. Passez en revue les associations de files d'attente, puis sélectionnez Suivant.
19. (Facultatif) Pour l'environnement de file d'attente Conda par défaut, nous créerons un environnement pour votre file d'attente qui installera les packages Conda demandés par les jobs.

> **Note**
>
> L'environnement de file d'attente Conda est utilisé pour installer les packages Conda demandés par les jobs. Généralement, vous devez décocher l'environnement de file d'attente Conda sur les files d'attente associées aux CMF, car les commandes Conda requises ne seront pas installées par défaut dans les CMF.

20. (Facultatif) Ajoutez des balises à votre CMF. Pour plus d'informations, consultez la section Marquage de vos AWS ressources.
21. Passez en revue la configuration de votre flotte et apportez les modifications nécessaires.
22. Choisissez Create fleet (Créer une flotte).
23. Sélectionnez l'onglet Flottes, puis notez l'ID de flotte.

AWS CLI

Pour utiliser le AWS CLI pour créer une flotte gérée par le client

1. Ouvrez le AWS CLI.
2. Modification `fleet-trust-policy.json`.
    a. Ajoutez la politique IAM suivante, en remplaçant le texte en *ITALIQUE* par votre identifiant de AWS compte et l'identifiant de ferme 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. Enregistrez vos modifications.

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

   a. Ajoutez la politique IAM suivante.

```
{
    "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. Enregistrez vos modifications.

4. Ajoutez un rôle IAM que les employés de votre flotte pourront utiliser.

```
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. Modification `create-fleet-request.json`.

a. Ajoutez la politique IAM suivante, en remplaçant le texte en ITALIQUE par les valeurs de votre CMF.

> **Note**
>
> Vous pouvez trouver le *ROLE_ARN* dans le. `create-cmf-fleet.json`
> Pour *OS_FAMILY*, vous devez choisir l'une des `linux` options suivantes : ou. `macos` `windows`

```
{
    "farmId": "FARM_ID",
    "displayName": "FLEET_NAME",
    "description": "FLEET_DESCRIPTION",
    "roleArn": "ROLE_ARN",
    "minWorkerCount": 0,
    "maxWorkerCount": 10,
    "configuration": {
        "customerManaged": {
            "mode": "NO_SCALING",
            "workerCapabilities": {
                "vCpuCount": {
                    "min": 1,
                    "max": 4
                },
                "memoryMiB": {
                    "min": 1024,
                    "max": 4096
                },
                "osFamily": "OS_FAMILY",
                "cpuArchitectureType": "x86_64",
            },
        },
    }
}
```

b. Enregistrez vos modifications.

6. Créez votre flotte.

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

Configuration et configuration de l'hôte de travail

Un hôte de travail fait référence à une machine hôte qui exécute un serveur de travail Deadline Cloud. Cette section explique comment configurer l'hôte de travail et le configurer en fonction de vos besoins spécifiques. Chaque hôte de travail exécute un programme appelé agent de travail. L'agent des travailleurs est chargé de :

- Gérer le cycle de vie des travailleurs.
- Synchronisation du travail assigné, de son avancement et de ses résultats.
- Surveillance du travail en cours.
- Transfert des journaux vers des destinations configurées.

Nous vous recommandons d'utiliser l'agent de travail Deadline Cloud fourni. L'agent de travail est open source et nous encourageons les demandes de fonctionnalités, mais vous pouvez également les développer et les personnaliser en fonction de vos besoins.

Pour effectuer les tâches décrites dans les sections suivantes, vous avez besoin des éléments suivants :

Linux

- Une Linux instance basée sur Amazon Elastic Compute Cloud (Amazon EC2). Nous recommandons Amazon Linux 2023.
- `sudo`privilèges.
- Python 3.9 ou supérieur.

Windows

- Une Windows instance basée sur Amazon Elastic Compute Cloud (Amazon EC2). Nous recommandons Windows Server 2022
- Accès administrateur à l'hôte du travailleur
- Python 3.9 ou supérieur installé pour tous les utilisateurs

Création et configuration d'un environnement virtuel Python

Vous pouvez créer un environnement virtuel Python Linux si vous avez installé Python 3.9 ou supérieur et que vous l'avez placé dans votre`PATH`.

Pour créer et activer un environnement virtuel Python

1. Ouvrez le AWS CLI.
2. Créez et activez un environnement virtuel Python.

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

Installer l'agent de travail de Deadline Cloud

Après avoir configuré votre Python et créé un environnement virtuel sur celui-ciLinux, installez les packages Python de l'agent de travail Deadline Cloud.

Pour installer les packages Python de l'agent de travail

1. Ouvrez un terminal .
   a. LinuxActivé, ouvrez un terminal en tant qu'`root`utilisateur (ou utilisez`sudo`/`su`)
   b. ActivéWindows, ouvrez une invite de commande ou un PowerShell terminal d'administrateur.
2. Téléchargez et installez les packages d'agents de travail de Deadline Cloud depuis PyPI :

> **Note**
>
> ActivéWindows, les fichiers de l'agent doivent être installés dans le répertoire global site-packages de Python. Les environnements virtuels Python ne sont actuellement pas pris en charge.

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

Configuration de l'agent de travail Deadline Cloud

Vous pouvez configurer les paramètres de l'agent de travail de Deadline Cloud de trois manières. Nous vous recommandons d'utiliser le système d'exploitation configuré via`install-deadline-worker`.

Arguments de ligne de commande — Vous pouvez spécifier des arguments lorsque vous exécutez l'agent de travail Deadline Cloud depuis la ligne de commande. Certains paramètres de configuration ne sont pas disponibles via les arguments de la ligne de commande. Pour voir tous les arguments de ligne de commande disponibles, entrez `deadline-worker-agent --help` pour voir tous les arguments de ligne de commande disponibles.

Variables d'environnement — Vous pouvez configurer l'agent de travail de Deadline Cloud en définissant une variable d'environnement commençant par`DEADLINE_WORKER_`. Par exemple, vous pouvez l'utiliser `export DEADLINE_WORKER_VERBOSE=true` pour définir la sortie de l'agent de travail sur détaillée. Pour plus d'exemples et d'informations, reportez-vous à `/etc/amazon/deadline/worker.toml.example` la section sur Linux ou `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` surWindows.

Fichier de configuration : lorsque vous installez l'agent de travail, celui-ci crée un fichier de configuration situé à l'emplacement `/etc/amazon/deadline/worker.toml` activé Linux ou `C:\ProgramData\Amazon\Deadline\Config\worker.toml` activéWindows. L'agent de travail charge ce fichier de configuration au démarrage. Vous pouvez utiliser l'exemple de fichier de configuration (`/etc/amazon/deadline/worker.toml.example`activé Linux ou `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` activéWindows) pour adapter le fichier de configuration de l'agent de travail par défaut à vos besoins spécifiques.

Enfin, nous vous recommandons d'activer l'arrêt automatique pour l'agent de travail. Cela permet au parc de travailleurs d'augmenter en cas de besoin et de s'arrêter une fois le travail de rendu terminé. La mise à l'échelle automatique vous permet de vous assurer que vous n'utilisez les ressources que lorsque vous en avez besoin.

Pour activer l'arrêt automatique

En tant qu'**`root`**utilisateur :

- Installez l'agent de travail avec des paramètres**`--allow-shutdown`**.

Linux

Entrez :

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

Windows

Entrez :

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

Création de groupes et d'utilisateurs de tâches

Cette section décrit la relation utilisateur/groupe requise entre l'utilisateur agent et les utilisateurs `jobRunAsUser` définis dans vos files d'attente.

L'agent de travail de Deadline Cloud doit s'exécuter en tant qu'utilisateur dédié spécifique à l'agent sur l'hôte. Vous devez configurer la `jobRunAsUser` propriété des files d'attente de Deadline Cloud afin que les utilisateurs exécutent les tâches de file d'attente en tant qu'utilisateur et groupe de système d'exploitation spécifiques. Cela signifie que vous pouvez contrôler les autorisations de système de fichiers partagés dont disposent vos tâches. Il constitue également une limite de sécurité importante entre vos tâches et l'utilisateur de l'agent de travail.

Linuxutilisateurs et groupes d'emplois

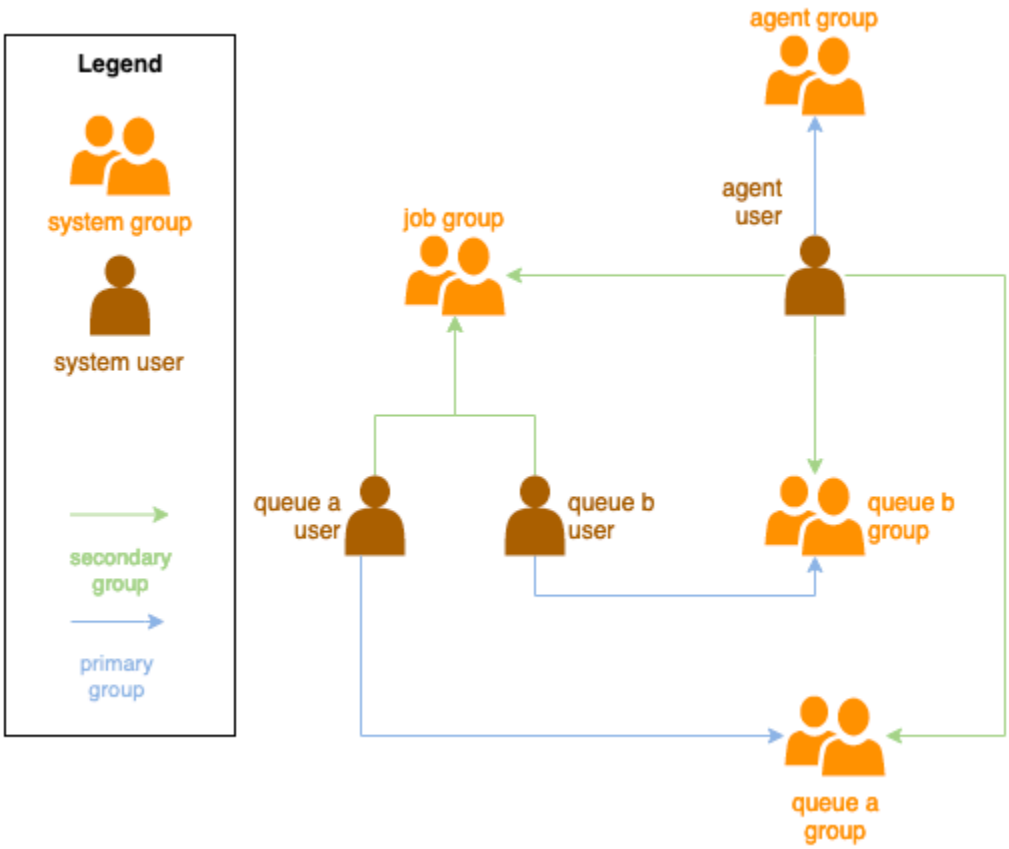
Pour configurer votre agent-utilisateur et `jobRunAsUser` vérifier que vous répondez aux exigences suivantes :

- Il existe un groupe pour chacun`jobRunAsUser`, et c'est le groupe principal pour le groupe correspondant`jobRunAsUser`.

- L'agent-utilisateur appartient au groupe principal des quatre files d'attente où le travailleur obtient du travail. `jobRunAsUser` Pour les meilleures pratiques en matière de sécurité, nous recommandons ce groupe en tant que groupe secondaire de l'agent-utilisateur. Ce groupe partagé permet à l'agent de travail de rendre les fichiers disponibles pour la tâche pendant son exécution.
- A `jobRunAsUser` n'appartient pas au groupe principal de l'agent-utilisateur. Pour connaître les meilleures pratiques en matière de sécurité :
  - Les fichiers sensibles écrits par l'agent de travail appartiennent au groupe principal de l'agent.
  - Si a `jobRunAsUser` appartient à ce groupe et que les fichiers écrits par l'agent de travail peuvent être accessibles par les tâches soumises à la file d'attente exécutée sur le travailleur.
- La AWS région par défaut doit correspondre à la région de la ferme à laquelle appartient le travailleur. Pour plus d'informations, consultez Configuration et paramètres des fichiers d'identification.

  Cela devrait être appliqué à :
  - L'agent-utilisateur
  - Tous les `jobRunAsUser` comptes de file d'attente du travailleur
- L'agent-utilisateur peut exécuter des `sudo` commandes en tant que. `jobRunAsUser`

Le schéma suivant illustre la relation entre l'utilisateur de l'agent et les `jobRunAsUser` utilisateurs et groupes pour les files d'attente associées à la flotte.



Utilisateurs Windows

Pour utiliser un Windows utilisateur en tant que`jobRunAsUser`, celui-ci doit répondre aux exigences suivantes :

- Tous les `jobRunAsUser` utilisateurs de la file d'attente doivent exister.
- Leurs mots de passe doivent correspondre à la valeur du secret spécifiée dans le `JobRunAsUser` champ de leur file d'attente. Pour obtenir des instructions, reportez-vous à l'étape 7 deCréer une file d'attente.
- L'agent-utilisateur doit être en mesure de se connecter sous le nom de ces utilisateurs.

Gérer l'accès aux secrets des utilisateurs de Windows Job

Lorsque vous configurez une file d'attente sous Windows`jobRunAsUser`, vous devez spécifier un secret du Gestionnaire de AWS Secrets. La valeur de ce secret est censée être un objet codé en JSON de la forme suivante :

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

Pour que les travailleurs puissent exécuter des tâches conformément à la configuration de la file d'attente`jobRunAsUser`, le rôle IAM de la flotte doit disposer des autorisations nécessaires pour obtenir la valeur du secret. Si le secret est chiffré à l'aide d'une clé KMS gérée par le client, le rôle IAM de la flotte doit également être autorisé à le déchiffrer à l'aide de la clé KMS.

Il est fortement recommandé de suivre le principe du moindre privilège pour ces secrets. Cela signifie que l'accès pour récupérer la valeur secrète du `jobRunAsUser` → `windows` → d'une file d'attente `passwordArn` doit être :

- attribué à un rôle de flotte lorsqu'une association de flotte de files d'attente est créée entre la flotte et la file d'attente
- révoqué d'un rôle de flotte lorsqu'une association de file d'attente et de flotte est supprimée entre le parc et la file d'attente

De plus, le secret du AWS Secrets Manager contenant le `jobRunAsUser` mot de passe doit être supprimé lorsqu'il n'est plus utilisé.

Autoriser l'accès à un mot de passe secret

Les flottes Deadline Cloud ont besoin d'accéder au `jobRunAsUser` mot de passe stocké dans le secret de mot de passe de la file d'attente lorsque la file d'attente et la flotte sont associées. Nous vous recommandons d'utiliser la politique de ressources de AWS Secrets Manager pour accorder l'accès aux rôles de la flotte. Si vous respectez strictement cette directive, il est plus facile de déterminer quels rôles de flotte ont accès au secret.

Pour autoriser l'accès au secret

1. Ouvrez la console AWS Secret Manager pour accéder au secret.
2. Dans la section « Autorisations relatives aux ressources », ajoutez une déclaration de politique sous la forme suivante :

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

```
    {
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "FLEET_ROLE_ARN"
      },
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    // ...
  ]
}
```

Révoquer l'accès à un mot de passe secret

Lorsqu'une flotte n'a plus besoin d'accéder à une file d'attente, supprimez l'accès au mot de passe secret de la file d'attente`jobRunAsUser`. Nous vous recommandons d'utiliser la politique de ressources de AWS Secrets Manager pour accorder l'accès aux rôles de la flotte. Si vous respectez strictement cette directive, il est plus facile de déterminer quels rôles de flotte ont accès au secret.

Pour révoquer l'accès au secret

1. Ouvrez la console AWS Secret Manager pour accéder au secret.
2. Dans la section Autorisations relatives aux ressources, supprimez la déclaration de politique du formulaire :

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

Installation et configuration du logiciel requis pour les tâches

Après avoir configuré l'agent de travail Deadline Cloud, vous pouvez préparer l'hôte de travail avec tous les logiciels nécessaires à l'exécution des tâches.

Lorsque vous soumettez une tâche à une file d'attente associée`jobRunAsUser`, la tâche s'exécute sous le nom de cet utilisateur. Toutes les commandes doivent être disponibles dans le `PATH` fichier de cet utilisateur.

Sous Linux, vous pouvez spécifier le `PATH` pour un utilisateur dans l'une des options suivantes :

- leur `~/.bashrc` ou `~/.bash_profile`
- fichiers de configuration système tels que `/etc/profile.d/*` et `/etc/profile`
- scripts de démarrage du shell :`/etc/bashrc`.

Sous Windows, vous pouvez spécifier le `PATH` pour un utilisateur dans l'une des options suivantes :

- leurs variables d'environnement spécifiques à l'utilisateur
- les variables d'environnement à l'échelle du système

Installation d'adaptateurs d'outils de création de contenu numérique

Deadline Cloud fournit des applications de création de contenu numérique (DCC) avec un support d'intégration de premier niveau. Pour utiliser ces intégrations sur un parc géré par le client, vous devez installer le logiciel DCC et les adaptateurs.

Pour installer des adaptateurs DCC sur un parc géré par le client

1. Ouvrez le terminal A.
    a. Sous Linux, ouvrez un terminal en tant qu'`root`utilisateur (ou utilisez`sudo`/`su`)
    b. Sous Windows, ouvrez une invite de commande ou un PowerShell terminal d'administrateur.
2. Installez les packages d'adaptateurs Deadline Cloud.

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

Configuration des AWS informations d'identification

Cette section explique comment configurer les AWS informations d'identification.

Cette phase initiale du cycle de vie des travailleurs est en train de démarrer. Au cours de cette phase, le logiciel d'agent des travailleurs crée un travailleur dans votre flotte et obtient les AWS informations d'identification du rôle de votre flotte pour une exploitation ultérieure.

AWS credentials for Amazon EC2

Pour configurer les AWS informations d'identification pour Amazon EC2

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Sélectionnez Rôles dans le volet de navigation, puis Créer un rôle.
3. Sélectionnez le AWS service.
4. Sélectionnez EC2 comme service ou cas d'utilisation, puis sélectionnez Suivant.
5. Joignez la politique `AWSDeadlineCloud-WorkerHost` AWS gérée.

On-premise AWS credentials

Pour configurer les informations AWS d'identification sur site

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Sélectionnez Rôles dans le volet de navigation, puis Créer un rôle.
3. Sélectionnez Compte AWS, puis sélectionnez Suivant.
4. Joignez la politique `AWSDeadlineCloud-WorkerHost` AWS gérée.
5. Générez un accès AWS IAM et des clés secrètes pour l'utilisateur IAM :
   a. Pour IAM Role Anywhere, voir IAM Roles Anywhere.
   b. Pour connaître le moyen le plus sûr de configurer les informations d'identification sur l'hôte, consultez la section Obtention d'informations d'identification de sécurité temporaires auprès d'AWS Identity and Access Management Roles Anywhere.
   c. Vous pouvez également utiliser la CLI comme alternative d'authentification. Pour plus d'informations, voir Authentifier avec les informations d'identification utilisateur IAM.
6. Stockez ces clés dans le fichier d'informations d' AWS identification de l'agent-utilisateur sur le système de fichiers hôte du travail.

a. Sous Linux, il se trouve à l'adresse `~/.aws/credentials`

b. Sous Windows, il se trouve à l'adresse `%USERPROFILE%\.aws\credentials`

> **Note**
>
> Les informations d'identification ne doivent être accessibles que par le nom d'utilisateur du système d'exploitation (`deadline-worker-agent`) qui a installé l'agent de travail.

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

7. Modifiez le `deadline-worker-agent` propriétaire et les autorisations.

> **Note**
>
> Si vous avez modifié le nom d'utilisateur du système d'exploitation (`deadline-worker-agent`) lors de l'installation de l'agent de travail, utilisez plutôt ce nom.

Créer un Amazon Machine Image

Pour créer un Amazon Machine Image (AMI) à utiliser dans une flotte gérée par le client (CMF) Amazon Elastic Compute Cloud (Amazon EC2), effectuez les tâches décrites dans cette section. Vous devez créer une instance Amazon EC2 avant de continuer. Pour plus d'informations, consultez Lancer votre instance dans le guide de l'utilisateur Amazon EC2 pour les instances Linux.

> **Important**
>
> La création d'un instantané des volumes attachés à l'instance Amazon EC2 est AMI créé. Tout logiciel installé sur l'instance est conservé, donc les instances, qui sont réutilisées lorsque vous lancez des instances depuis leAMI. Nous vous recommandons d'adopter une

stratégie de correction et de mettre régulièrement à jour tout nouveau AMI logiciel avant de l'appliquer à votre flotte.

Préparez l'instance Amazon EC2

Avant de créer unAMI, vous devez supprimer l'état de travail. L'état du travailleur persiste entre les lancements de l'agent de travail. Si cet état persisteAMI, toutes les instances lancées à partir de celui-ci partageront le même état.

Nous vous recommandons également de supprimer tous les fichiers journaux existants. Les fichiers journaux peuvent rester sur une instance Amazon EC2 lorsque vous préparez l'AMI. La suppression de ces fichiers permet de réduire la confusion lors du diagnostic d'un éventuel problème dans les flottes de travailleurs qui utilisent l'AMI.

Vous devez également activer le service système d'agent de travail afin que l'agent de travail Deadline Cloud soit lancé au démarrage d'Amazon EC2.

Enfin, nous vous recommandons d'activer l'arrêt automatique de l'agent de travail. Cela permet au parc de travailleurs d'augmenter en cas de besoin et de s'arrêter une fois le travail de rendu terminé. Cette mise à l'échelle automatique permet de s'assurer que vous n'utilisez les ressources que lorsque vous en avez besoin.

Pour préparer l'instance Amazon EC2

1. Ouvrez la console Amazon EC2.
2. Lancez une instance Amazon EC2. Pour plus d'informations, consultez Lancer votre instance.
3. Configurez l'hôte pour qu'il se connecte à votre fournisseur d'identité (IdP), puis montez le système de fichiers partagé dont il a besoin.
4. Suivez les didacticiels pourInstaller l'agent de travail de Deadline Cloud, puisConfiguration de l'agent de travail, etCréation de groupes et d'utilisateurs de tâches.
5. Si vous préparez un logiciel AMI basé sur Amazon Linux 2023 pour exécuter un logiciel compatible avec la plate-forme de référence VFX, vous devez mettre à jour plusieurs exigences. Pour plus d'informations, veuillez consulter Compatibilité VFX Reference Platform.
6. Ouvrez un terminal .
    a. Sous Linux, ouvrez un terminal en tant qu'`root`utilisateur (ou utilisez`sudo`/`su`)

b. Sous Windows, ouvrez une invite de commande ou un PowerShell terminal d'administrateur.

7. Assurez-vous que le service de travail n'est pas en cours d'exécution et qu'il est configuré pour démarrer au démarrage :

   a. Sous Linux, exécutez

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

   b. Sous Windows, exécutez

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

8. Supprimez l'état du travailleur.

   a. Sous Linux, exécutez

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

   b. Sous Windows, exécutez

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

9. Supprimez les fichiers journaux.

   a. Sous Linux, exécutez

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

   b. Sous Windows, exécutez

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

10. Sous Windows, il est recommandé d'exécuter l'application Amazon EC2Launch Settings qui se trouve dans le menu Démarrer pour terminer la préparation finale de l'hôte et arrêter l'instance.

> **Note**
>
> Vous DEVEZ choisir Shutdown without Sysprep et ne jamais choisir Shutdown with Sysprep. L'arrêt de Sysprep rendra tous les utilisateurs locaux inutilisables. Pour plus

d'informations, consultez la section Avant de commencer de la rubrique Création d'une AMI personnalisée du Guide de l'utilisateur pour les instances Windows.

Construisez le AMI

Pour construire le AMI

1. Ouvrez la console Amazon EC2.
2. Sélectionnez Instances dans le volet de navigation, puis sélectionnez votre instance.
3. Choisissez État de l'instance, puis Arrêter l'instance.
4. Une fois l'instance arrêtée, choisissez Actions.
5. Choisissez Image et modèles, puis Créer une image.
6. Entrez le nom de l'image.
7. (Facultatif) Entrez une description pour votre image.
8. Choisissez Create image (Créer une image).

Créez une infrastructure de flotte avec un groupe Amazon EC2 Auto Scaling

Cette section explique comment créer une flotte Amazon EC2 Auto Scaling.

Utilisez le modèle AWS CloudFormation YAML ci-dessous pour créer un groupe Amazon EC2 Auto Scaling (Auto Scaling), un Amazon Virtual Private Cloud (Amazon VPC) avec deux sous-réseaux, un profil d'instance et un rôle d'accès à l'instance. Ils sont nécessaires pour lancer une instance à l'aide d'Auto Scaling dans les sous-réseaux.

Vous devez revoir et mettre à jour la liste des types d'instances en fonction de vos besoins de rendu.

Pour créer une flotte Amazon EC2 Auto Scaling

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Créez un CloudFormation modèle avec des paramètres `Farm ID`Fleet `ID`, et`AMI ID`.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Amazon Deadline Cloud customer-managed fleet
```

```
Parameters:
  FarmId:
    Type: String
    Description: Farm ID
  FleetId:
    Type: String
    Description: Fleet ID
  AMIId:
    Type: String
    Description: AMI ID for launcing Workers
Resources:
  deadlineVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: 100.100.0.0/16
  deadlineWorkerSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: !Join
        - ' '
        - - Security Group created for deadline workers in fleet
          - !Ref FleetId
      GroupName: !Join
        - ''
        - - deadlineWorkerSecurityGroup-
          - !Ref FleetId
      SecurityGroupEgress:
        - CidrIp: 0.0.0.0/0
          IpProtocol: '-1'
      SecurityGroupIngress: []
      VpcId: !Ref deadlineVPC
  deadlineIGW:
    Type: 'AWS::EC2::InternetGateway'
    Properties: {}
  deadlineVPCGatewayAttachment:
    Type: 'AWS::EC2::VPCGatewayAttachment'
    Properties:
      VpcId: !Ref deadlineVPC
      InternetGatewayId: !Ref deadlineIGW
  deadlinePublicRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref deadlineVPC
  deadlinePublicRoute:
```

```
    Type: 'AWS::EC2::Route'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref deadlineIGW
    DependsOn:
      - deadlineIGW
      - deadlineVPCGatewayAttachment
  deadlinePublicSubnet0:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref deadlineVPC
      CidrBlock: 100.100.16.0/22
      AvailabilityZone: !Join
        - ''
        - - !Ref 'AWS::Region'
          - a
  deadlineSubnetRouteTableAssociation0:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      SubnetId: !Ref deadlinePublicSubnet0
  deadlinePublicSubnet1:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref deadlineVPC
      CidrBlock: 100.100.20.0/22
      AvailabilityZone: !Join
        - ''
        - - !Ref 'AWS::Region'
          - c
  deadlineSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      SubnetId: !Ref deadlinePublicSubnet1
  deadlineInstanceAccessAccessRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Join
        - '-'
        - - deadline
          - InstanceAccess
          - !Ref FleetId
```

```
    AssumeRolePolicyDocument:
      Statement:
        - Effect: Allow
          Principal:
            Service: ec2.amazonaws.com
          Action:
            - 'sts:AssumeRole'
    Path: /
    ManagedPolicyArns:
      - 'arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy'
      - 'arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore'
      - 'arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost'
deadlineInstanceProfile:
  Type: 'AWS::IAM::InstanceProfile'
  Properties:
    Path: /
    Roles:
      - !Ref deadlineInstanceAccessAccessRole
deadlineLaunchTemplate:
  Type: 'AWS::EC2::LaunchTemplate'
  Properties:
    LaunchTemplateName: !Join
      - ''
      - - deadline-LT-
        - !Ref FleetId
    LaunchTemplateData:
      NetworkInterfaces:
        - DeviceIndex: 0
          AssociatePublicIpAddress: true
          Groups:
            - !Ref deadlineWorkerSecurityGroup
          DeleteOnTermination: true
      ImageId: !Ref AMIId
      InstanceInitiatedShutdownBehavior: terminate
      IamInstanceProfile:
        Arn: !GetAtt
          - deadlineInstanceProfile
          - Arn
      MetadataOptions:
        HttpTokens: required
        HttpEndpoint: enabled

deadlineAutoScalingGroup:
  Type: 'AWS::AutoScaling::AutoScalingGroup'
```

```
    Properties:
      AutoScalingGroupName: !Join
        - ''
        - - deadline-ASG-autoscalable-
          - !Ref FleetId
      MinSize: 0
      MaxSize: 10
      VPCZoneIdentifier:
        - !Ref deadlinePublicSubnet0
        - !Ref deadlinePublicSubnet1
      NewInstancesProtectedFromScaleIn: true
      MixedInstancesPolicy:
        InstancesDistribution:
          OnDemandBaseCapacity: 0
          OnDemandPercentageAboveBaseCapacity: 0
          SpotAllocationStrategy: capacity-optimized
          OnDemandAllocationStrategy: lowest-price
        LaunchTemplate:
          LaunchTemplateSpecification:
            LaunchTemplateId: !Ref deadlineLaunchTemplate
            Version: !GetAtt
              - deadlineLaunchTemplate
              - LatestVersionNumber
          Overrides:
            - InstanceType: m5.large
            - InstanceType: m5d.large
            - InstanceType: m5a.large
            - InstanceType: m5ad.large
            - InstanceType: m5n.large
            - InstanceType: m5dn.large
            - InstanceType: m4.large
            - InstanceType: m3.large
            - InstanceType: r5.large
            - InstanceType: r5d.large
            - InstanceType: r5a.large
            - InstanceType: r5ad.large
            - InstanceType: r5n.large
            - InstanceType: r5dn.large
            - InstanceType: r4.large
      MetricsCollection:
        - Granularity: 1Minute
          Metrics:
            - GroupMinSize
            - GroupMaxSize
```

```
            - GroupDesiredCapacity
            - GroupInServiceInstances
            - GroupTotalInstances
            - GroupInServiceCapacity
            - GroupTotalCapacity
```

3. Après avoir créé les rôles IAM, vous devez prendre connaissance des points suivants :

   - Les informations d'identification du rôle IAM associées à l'instance Amazon EC2 de votre travailleur sont disponibles pour tous les processus exécutés sur ce travailleur, y compris les tâches. Le travailleur doit avoir le moins de privilèges pour opérer : `deadline:CreateWorker` et `deadline:AssumeFleetRoleForWorker.`
   - L'agent de travail obtient les informations d'identification pour le rôle de file d'attente et les configure pour les utiliser lors de l'exécution de tâches. Le rôle de profil d'instance Amazon EC2 ne doit pas inclure les autorisations nécessaires à vos tâches.

Faites évoluer automatiquement votre flotte Amazon EC2 grâce à la fonction de recommandation de dimensionnement de Deadline Cloud

Deadline Cloud utilise un groupe Amazon EC2 Auto Scaling (Auto Scaling) pour dimensionner automatiquement le parc géré par le client (CMF) Amazon EC2. Vous devez configurer le mode flotte et déployer l'infrastructure requise dans votre compte afin de faire évoluer votre flotte automatiquement. L'infrastructure que vous avez déployée fonctionnera pour toutes les flottes, vous ne devez donc la configurer qu'une seule fois.

Le flux de travail de base est le suivant : vous configurez le mode flotte pour qu'il évolue automatiquement, puis Deadline Cloud envoie un EventBridge événement pour cette flotte chaque fois que la taille recommandée change (un événement contient l'identifiant de la flotte, la taille de flotte recommandée et d'autres métadonnées). Vous aurez une EventBridge règle pour filtrer les événements pertinents et disposerez d'un Lambda pour les consommer. Le Lambda s'intégrera à Amazon EC2 `AutoScalingGroup` Auto Scaling pour dimensionner automatiquement le parc Amazon EC2.

Réglez le mode flotte sur **`EVENT_BASED_AUTO_SCALING`**

Configurez votre mode flotte pour`EVENT_BASED_AUTO_SCALING`. Pour ce faire, vous pouvez utiliser la console ou utiliser le AWS CLI pour appeler directement l'`UpdateFleet`API `CreateFleet` or. Une fois le mode configuré, Deadline Cloud commence à envoyer EventBridge des événements chaque fois que la taille de flotte recommandée change.

- Exemple de `UpdateFleet` commande :

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

- Exemple de `CreateFleet` commande :

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

Voici un exemple d'`configuration.json`utilisation dans les commandes CLI ci-dessus (`--configuration file://configuration.json`).

- Pour activer Auto Scaling sur votre flotte, vous devez régler le mode sur`EVENT_BASED_AUTO_SCALING`.
- `workerCapabilities`Il s'agit des valeurs par défaut attribuées au CMF lorsque vous l'avez créé. Vous pouvez modifier ces valeurs si vous avez besoin d'augmenter les ressources disponibles pour votre CMF.

Après avoir configuré le mode flotte, Deadline Cloud commence à émettre des événements de recommandation de taille de flotte pour cette flotte.

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

```
            "cpuArchitectureType": "x86_64",
        }
    }
}
```

Déployez la pile Auto Scaling à l'aide du AWS CloudFormation modèle

Vous pouvez configurer une EventBridge règle pour filtrer les événements, un Lambda pour consommer les événements et contrôler Auto Scaling, et une file d'attente SQS pour stocker les événements non traités. Utilisez le AWS CloudFormation modèle suivant pour déployer tous les éléments d'une pile. Une fois les ressources déployées avec succès, vous pouvez soumettre une tâche et la flotte augmentera automatiquement.

```
Resources:
  AutoScalingLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
        ZipFile: |-
          """
          This lambda is configured to handle "Fleet Size Recommendation Change"
          messages. It will handle all such events, and requires
          that the ASG is named based on the fleet id. It will scale up/down the fleet
          based on the recommended fleet size in the message.

          Example EventBridge message:
          {
              "version": "0",
              "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
              "detail-type": "Fleet Size Recommendation Change",
              "source": "aws.deadline",
              "account": "111122223333",
              "time": "2017-12-22T18:43:48Z",
              "region": "us-west-1",
              "resources": [],
              "detail": {
                  "farmId": "farm-12345678900000000000000000000000",
                  "fleetId": "fleet-12345678900000000000000000000000",
                  "oldFleetSize": 1,
                  "newFleetSize": 5,
              }
          }
          """
```

```
          import json
          import boto3
          import logging

          logger = logging.getLogger()
          logger.setLevel(logging.INFO)

          auto_scaling_client = boto3.client("autoscaling")

          def lambda_handler(event, context):
              logger.info(event)
              event_detail = event["detail"]
              fleet_id = event_detail["fleetId"]
              desired_capacity = event_detail["newFleetSize"]

              asg_name = f"deadline-ASG-autoscalable-{fleet_id}"
              auto_scaling_client.set_desired_capacity(
                  AutoScalingGroupName=asg_name,
                  DesiredCapacity=desired_capacity,
                  HonorCooldown=False,
              )

              return {
                  'statusCode': 200,
                  'body': json.dumps(f'Successfully set desired_capacity for {asg_name}
to {desired_capacity}')
              }
      Handler: index.lambda_handler
      Role: !GetAtt
        - AutoScalingLambdaServiceRole
        - Arn
      Runtime: python3.11
    DependsOn:
      - AutoScalingLambdaServiceRoleDefaultPolicy
      - AutoScalingLambdaServiceRole
  AutoScalingEventRule:
    Type: 'AWS::Events::Rule'
    Properties:
      EventPattern:
        source:
          - aws.deadline
        detail-type:
          - Fleet Size Recommendation Change
```

```
      State: ENABLED
      Targets:
        - Arn: !GetAtt
            - AutoScalingLambda
            - Arn
          DeadLetterConfig:
            Arn: !GetAtt
              - UnprocessedAutoScalingEventQueue
              - Arn
          Id: Target0
          RetryPolicy:
            MaximumRetryAttempts: 15
  AutoScalingEventRuleTargetPermission:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !GetAtt
        - AutoScalingLambda
        - Arn
      Principal: events.amazonaws.com
      SourceArn: !GetAtt
        - AutoScalingEventRule
        - Arn
  AutoScalingLambdaServiceRole:
    Type: 'AWS::IAM::Role'
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: 'sts:AssumeRole'
            Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
        Version: 2012-10-17
      ManagedPolicyArns:
        - !Join
          - ''
          - - 'arn:'
            - !Ref 'AWS::Partition'
            - ':iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
  AutoScalingLambdaServiceRoleDefaultPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyDocument:
        Statement:
```

```
          - Action: 'autoscaling:SetDesiredCapacity'
            Effect: Allow
            Resource: '*'
        Version: 2012-10-17
      PolicyName: AutoScalingLambdaServiceRoleDefaultPolicy
      Roles:
        - !Ref AutoScalingLambdaServiceRole
  UnprocessedAutoScalingEventQueue:
    Type: 'AWS::SQS::Queue'
    Properties:
      QueueName: deadline-unprocessed-autoscaling-events
    UpdateReplacePolicy: Delete
    DeletionPolicy: Delete
  UnprocessedAutoScalingEventQueuePolicy:
    Type: 'AWS::SQS::QueuePolicy'
    Properties:
      PolicyDocument:
        Statement:
          - Action: 'sqs:SendMessage'
            Condition:
              ArnEquals:
                'aws:SourceArn': !GetAtt
                  - AutoScalingEventRule
                  - Arn
            Effect: Allow
            Principal:
              Service: events.amazonaws.com
            Resource: !GetAtt
              - UnprocessedAutoScalingEventQueue
              - Arn
        Version: 2012-10-17
      Queues:
        - !Ref UnprocessedAutoScalingEventQueue
```

Connectez les flottes gérées par le client à un point de terminaison de licence

Le serveur de licences basé sur l'utilisation de AWS Deadline Cloud (Deadline Cloud) fournit des licences à la demande pour certains produits tiers. Cela vous permet de payer au fur et à mesure. Vous n'êtes changé que pour le temps que vous utilisez.

Le serveur de licences basé sur l'utilisation de Deadline Cloud peut être utilisé avec n'importe quel type de flotte, à condition que les employés de Deadline Cloud puissent communiquer avec le serveur de licences. Ceci est automatiquement configuré dans les flottes gérées par le service. Cette configuration n'est nécessaire que pour les flottes gérées par le client.

Pour créer le serveur de licences, vous avez besoin des éléments suivants :

- Un groupe de sécurité pour le VPC de votre ferme qui autorise le trafic pour les licences tierces.
- Rôle AWS Identity and Access Management (IAM) associé à une politique qui permet d'accéder aux opérations du point de terminaison de la licence Deadline Cloud.

Rubriques

Étape 1 : créer un groupe de sécurité

Utilisez la console Amazon VPC (https://console.aws.amazon.com/vpc/) pour créer un groupe de sécurité pour le VPC de votre ferme. Configurez le groupe de sécurité pour autoriser les règles entrantes suivantes :

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

La source de chaque règle entrante est le groupe de sécurité des employés de la flotte.

Pour plus d'informations sur la création d'un groupe de sécurité, consultez la section Créer un groupe de sécurité dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Étape 2 : configurer le point de terminaison de licence

Un point de terminaison de licence fournit un accès aux serveurs de licences pour les produits tiers. Les demandes de licence sont envoyées au point de terminaison de licence. Le point de terminaison

les achemine vers le serveur de licences approprié. Le serveur de licences suit les limites d'utilisation et les droits. Des frais sont facturés pour chaque point de terminaison de licence que vous créez. Pour plus d'informations, veuillez consulter Tarification Amazon VPC.

Vous pouvez créer votre point de terminaison de licence à partir du AWS Command Line Interface avec les autorisations appropriées. Pour connaître la politique requise pour créer un point de terminaison de licence, voir Politique autorisant la création d'un point de terminaison de licence.

Vous pouvez utiliser l'environnement AWS CloudShell (https://console.aws.amazon.com/cloudshell/) ou tout autre AWS CLI environnement pour configurer le point de terminaison de licence à l'aide des AWS Command Line Interface commandes suivantes.

1. Créez le point de terminaison de licence. Remplacez l'ID du groupe de sécurité, l'ID de sous-réseau et l'ID VPC par les valeurs que vous avez créées précédemment. Si vous utilisez plusieurs sous-réseaux, séparez-les par des espaces.

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

2. Vérifiez que le point de terminaison a été créé avec succès à l'aide de la commande suivante. N'oubliez pas le nom DNS du point de terminaison VPC.

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

3. Consultez la liste des produits mesurés disponibles :

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

4. Ajoutez des produits mesurés au point de terminaison de licence à l'aide de la commande suivante.

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

Vous pouvez supprimer un produit d'un point de terminaison de licence à l'aide de la `remove-metered-product` commande suivante :

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

Vous pouvez supprimer un point de terminaison de licence à l'aide de la `delete-license-endpoint` commande suivante :

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

Étape 3 : Connecter une application de rendu à un point de terminaison

Une fois le point de terminaison de licence configuré, les applications l'utilisent de la même manière qu'elles utilisent un serveur de licences tiers. Vous configurez généralement le serveur de licences de l'application en définissant une variable d'environnement ou un autre paramètre système, tel qu'une clé de registre Microsoft Windows, sur un port et une adresse de serveur de licences.

Pour obtenir le nom DNS du point de terminaison de licence, utilisez la AWS CLI commande suivante.

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

Vous pouvez également utiliser la console Amazon VPC (https://console.aws.amazon.com/vpc/) pour identifier le point de terminaison VPC créé par l'API Deadline Cloud à l'étape précédente.

Exemples de configuration

Example — Autodesk Maya et Arnold

Définissez la variable d'environnement `ADSKFLEX_LICENSE_FILE` sur :

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

> **Note**
>
> Pour les Windows utilisateurs, utilisez un point-virgule (;) au lieu de deux points (:)) pour séparer les points de terminaison.

Example — Autodesk 3ds Max

Définissez la variable d'environnement `ADSKFLEX_LICENSE_FILE` sur :

```
2704@VPC_Endpoint_DNS_Name
```

Example — Foundry Nuke

Définissez la variable `foundry_LICENSE` d'environnement sur `6101@`*`VPC_Endpoint_DNS_Name`* Pour vérifier que les licences fonctionnent correctement, vous pouvez exécuter Nuke dans un terminal :

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

Example — SideFX Houdini, Mantra et Karma

Exécutez la commande suivante :

```
/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;"
```

Pour vérifier que les licences fonctionnent correctement, vous pouvez effectuer le rendu d'une scène Houdini à l'aide de cette commande :

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

Gestion des utilisateurs dans Deadline Cloud

AWS Deadline Cloud est utilisé AWS IAM Identity Center pour gérer les utilisateurs et les groupes. IAM Identity Center est un service d'authentification unique basé sur le cloud qui peut être intégré à votre fournisseur d'authentification unique (SSO) d'entreprise. Grâce à l'intégration, les utilisateurs peuvent se connecter avec leur compte d'entreprise.

Deadline Cloud active IAM Identity Center par défaut, et il est nécessaire pour configurer et utiliser Deadline Cloud. Pour plus d'informations, consultez Gérer votre source d'identité.

Le propriétaire de votre organisation AWS Organizations est chargé de gérer les utilisateurs et les groupes qui ont accès à votre moniteur Deadline Cloud. Vous pouvez créer et gérer ces utilisateurs et groupes à l'aide d'IAM Identity Center ou de la console Deadline Cloud. Pour plus d'informations, consultez What is AWS Organizations.

Vous créez et supprimez des utilisateurs et des groupes qui peuvent utiliser le moniteur pour gérer des fermes, des files d'attente et des flottes à l'aide de la console Deadline Cloud. Lorsque vous ajoutez un utilisateur à Deadline Cloud, il doit réinitialiser son mot de passe à l'aide d'IAM Identity Center avant d'y accéder.

Rubriques

Gérer les utilisateurs et les groupes pour le moniteur

Le propriétaire d'une organisation peut utiliser la console Deadline Cloud pour gérer les utilisateurs et les groupes ayant accès au moniteur Deadline Cloud. Vous pouvez choisir parmi les utilisateurs et les groupes IAM Identity Center existants, ou vous pouvez ajouter de nouveaux utilisateurs et groupes depuis la console.

1. Connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la. Sur la page principale, dans la section Commencer, choisissez Configurer Deadline Cloud ou Accéder au tableau de bord.
2. Dans le volet de navigation de gauche, choisissez Gestion des utilisateurs. Par défaut, l'onglet Groupes est sélectionné.

En fonction de l'action à effectuer, choisissez l'onglet Groupes ou l'onglet Utilisateurs.

Monitor groups

Pour créer un groupe

1. Choisissez Créer un groupe.
2. Entrez un nom de groupe. Le nom doit être unique parmi les groupes de votre organisation IAM Identity Center.

Pour supprimer un groupe

1. Sélectionnez le groupe à supprimer.
2. Sélectionnez Remove (Supprimer).
3. Dans la boîte de dialogue de confirmation, choisissez Supprimer le groupe.

> **Note**
>
> Vous supprimez le groupe d'IAM Identity Center. Les membres du groupe ne peuvent plus se connecter au Deadline Cloud ni accéder aux ressources de la ferme.

Monitor users

Pour ajouter des utilisateurs

1. Sélectionnez l'onglet Utilisateurs.
2. Sélectionnez Ajouter des utilisateurs.
3. Entrez le nom, l'adresse e-mail et le nom d'utilisateur du nouvel utilisateur.
4. Si vous le souhaitez, choisissez un ou plusieurs groupes IAM Identity Center auxquels ajouter le nouvel utilisateur.
5. Choisissez Envoyer une invitation pour envoyer au nouvel utilisateur un e-mail contenant des instructions pour rejoindre votre organisation IAM Identity Center.

Pour supprimer un utilisateur

1. Sélectionnez l'utilisateur que vous souhaitez supprimer de votre écran.

2. Sélectionnez Remove (Supprimer).
3. Dans la boîte de dialogue de confirmation, choisissez Supprimer l'utilisateur.

> **Note**
>
> Vous supprimez l'utilisateur d'IAM Identity Center. L'utilisateur ne peut plus se connecter au moniteur Deadline Cloud ni accéder aux ressources de la ferme.

Gérez les utilisateurs et les groupes pour les fermes, les files d'attente et les flottes

1. Si ce n'est pas déjà fait, connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la.
2. Dans le volet de navigation de gauche, sélectionnez Fermes et autres ressources.
3. Sélectionnez la ferme à gérer. Choisissez le nom de la ferme pour ouvrir la page de détails. Vous pouvez rechercher la ferme à l'aide de la barre de recherche.
4. Pour gérer une file d'attente ou un parc, choisissez l'onglet Files d'attente ou Flottes, puis choisissez la file d'attente ou le parc à gérer.
5. Choisissez l'onglet Gestion des accès. Par défaut, l'onglet Groupes est sélectionné. Pour gérer les utilisateurs, déplacez le bouton sur Utilisateurs.

En fonction de l'action à effectuer, choisissez l'onglet Groupes ou l'onglet Utilisateurs.

Pour les définitions des niveaux d'accès, consultez la section Autorisations.

Groups

Pour ajouter des groupes

1. Sélectionnez le bouton Groupes.
2. Choisissez Add Group (Ajouter un groupe).
3. Dans le menu déroulant, sélectionnez les groupes à ajouter.
4. Pour le niveau d'accès au groupe, choisissez l'une des options suivantes :

   - Lecteur

- Participant
- Directeur
- Propriétaire

5. Choisissez Ajouter.

Pour supprimer des groupes

1. Sélectionnez les groupes à supprimer.
2. Sélectionnez Remove (Supprimer).
3. Dans la boîte de dialogue de confirmation, sélectionnez Remove.

Users

Pour ajouter des utilisateurs

1. Pour ajouter un utilisateur, choisissez Ajouter un utilisateur.
2. Dans le menu déroulant, sélectionnez les utilisateurs à ajouter à votre ferme.
3. Pour le niveau d'accès utilisateur, choisissez l'une des options suivantes :

   - Lecteur
   - Participant
   - Directeur
   - Propriétaire

4. Choisissez Ajouter. Les utilisateurs sont ajoutés à votre ferme.

Pour supprimer des utilisateurs

1. Sélectionnez l'utilisateur à supprimer.
2. Dans la boîte de dialogue de confirmation de suppression, choisissez Supprimer. L'utilisateur est ensuite retiré de la ferme sélectionnée.

Vous pouvez également ajouter ou supprimer des autorisations de parc pour les utilisateurs et les groupes à l'aide de la console IAM Identity Center à l'adresse https://console.aws.amazon.com/singlesignon/.

Emplois chez Deadline Cloud

Une tâche est un ensemble d'instructions que AWS Deadline Cloud utilise pour planifier et exécuter le travail des employés disponibles. Lorsque vous créez une tâche, vous choisissez le parc et la file d'attente auxquels envoyer la tâche. Vous fournissez également un fichier JSON ou YAML qui fournit les instructions que les travailleurs doivent traiter. Deadline Cloud accepte les modèles de tâches conformes à la spécification Open Job Description (OpenJD) pour décrire les tâches. Pour plus d'informations, consultez la documentation Open Job Description sur le GitHub site Web.

Un emploi consiste à :

- Étapes — Définit le script à exécuter sur les travailleurs. Les étapes peuvent avoir des exigences telles qu'une mémoire de travail minimale ou d'autres étapes qui doivent d'abord être effectuées. Chaque étape comporte une ou plusieurs tâches.
- Tâches : unité de travail envoyée à un travailleur pour qu'il l'exécute. Une tâche est une combinaison du script d'une étape et des paramètres, tels que le numéro de trame, utilisés dans le script. La tâche est terminée lorsque toutes les tâches sont terminées pour toutes les étapes.
- Environnements — Configurez et démolissez des instructions partagées par plusieurs étapes ou tâches.

Vous pouvez créer une tâche de l'une des manières suivantes :

- Utilisez un émetteur Deadline Cloud.
- Créez un ensemble de tâches et utilisez l'interface de ligne de commande de Deadline Cloud (CLI de Deadline Cloud).
- Utilisez le AWS SDK.
- Utilisez le AWS Command Line Interface (AWS CLI).

Un soumissionnaire est un plugin pour votre logiciel de création de contenu numérique (DCC) qui gère la création d'une tâche dans l'interface de votre logiciel DCC. Après avoir créé la tâche, vous utilisez l'expéditeur pour l'envoyer à Deadline Cloud pour traitement. Dans les coulisses, l'auteur crée un modèle de tâche OpenJD qui décrit la tâche. Dans le même temps, il télécharge vos fichiers d'actifs dans un compartiment Amazon Simple Storage Service (Amazon S3). Pour réduire le temps nécessaire à l'envoi des fichiers, seuls les fichiers modifiés depuis le dernier chargement sont envoyés à Amazon S3.

Pour créer vos propres scripts et pipelines afin de soumettre des tâches à Deadline Cloud, vous pouvez utiliser la CLI de Deadline Cloud, le AWS SDK ou les opérations AWS CLI to call pour créer, obtenir, afficher et répertorier les tâches. Les rubriques suivantes expliquent comment utiliser la CLI de Deadline Cloud.

La CLI Deadline Cloud est installée en même temps que l'émetteur Deadline Cloud. Pour plus d'informations, consultez Configurer les soumissionnaires de Deadline Cloud.

Rubriques

- Soumission de tâches avec la CLI Deadline Cloud
- Planification des tâches dans Deadline Cloud
- États des tâches dans la CLI de Deadline Cloud
- Modifier des tâches dans Deadline Cloud
- Comment Deadline Cloud traite les tâches
- Résolution des problèmes liés à Deadline Cloud

Soumission de tâches avec la CLI Deadline Cloud

Pour soumettre une tâche à l'aide de l'interface de ligne de commande de Deadline Cloud (CLI de Deadline Cloud), utilisez la `deadline bundle submit` commande.

Les tâches sont soumises à des files d'attente. Si vous n'avez pas encore configuré de parc et de file d'attente, utilisez la console Deadline Cloud (https://console.aws.amazon.com/https://console.aws.amazon.com/deadlinecloud/home) pour configurer un parc et une file d'attente et pour voir le parc et l'ID de la file d'attente. Pour plus d'informations, voir Définir les détails du parc et Définir les détails de la file d'attente.

Pour définir le parc et la file d'attente par défaut pour la CLI de Deadline Cloud, utilisez la commande suivante. Lorsque vous définissez les valeurs par défaut, vous pouvez utiliser les commandes de la CLI de Deadline Cloud sans spécifier de parc ou de file d'attente. Dans l'exemple suivant, remplacez *`farmId`* et *`queueId`* par vos propres informations :

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

Pour spécifier les étapes et les tâches d'une tâche, créez un modèle de tâche OpenJD. Pour plus d'informations, consultez Template Schemas [Version : 2023-09] dans le référentiel de spécifications Open Job Description. GitHub

L'exemple suivant est un modèle de tâche YAML. Il définit un travail en deux étapes et cinq tâches par étape.

```
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
```

Pour créer une tâche, créez un nouveau dossier nommé`sample_job`, puis enregistrez le fichier modèle dans le nouveau dossier sous le nom`template.yaml`. Vous soumettez la tâche à l'aide de la commande Deadline Cloud CLI suivante :

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

La réponse de la commande contient un identifiant pour la tâche. N'oubliez pas l'identifiant afin de pouvoir vérifier le statut de la tâche ultérieurement.

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

Il existe des options supplémentaires que vous pouvez utiliser lorsque vous soumettez une offre d'emploi. Pour plus d'informations, consultez Plus d'options pour soumettre des tâches avec la CLI de Deadline Cloud.

Plus d'options pour soumettre des tâches avec la CLI de Deadline Cloud

La commande `deadline bundle submit` Deadline Cloud CLI fournit des options que vous pouvez utiliser pour spécifier des informations supplémentaires pour une tâche. Les exemples suivants montrent comment procéder pour :

- Spécifiez les paramètres utilisés lors du traitement du modèle de tâche.
- Joignez des fichiers et des dossiers dans un environnement partagé à une tâche.
- Définissez le nombre maximum d'échecs de tâches avant qu'une tâche ne soit annulée.
- Définissez le nombre maximum de tentatives pour une tâche.

Paramètres des tâches

L'`parameters`option définit la valeur d'un paramètre de tâche lorsque vous créez la tâche. Le modèle de tâche définit le champ et l'`parameters`option définit la valeur. Un paramètre peut avoir une valeur par défaut. Si une valeur est spécifiée pour le paramètre, elle remplace la valeur par défaut.

Le modèle de tâche suivant définit le `TestParameter` champ :

```
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
```

La commande suivante définit la valeur `TestParameter` de « Hello AWS » :

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

Profils de stockage

Les profils de stockage facilitent le partage de fichiers entre employés utilisant différents systèmes d'exploitation. Créez un profil de stockage à l'aide de la console Deadline Cloud. Utilisez ensuite le `storage-profile-id` paramètre pour utiliser le profil de stockage. Pour plus d'informations, consultez Stockage partagé dans Deadline Cloud.

Pour définir le profil de stockage pour les soumissions de tâches, à l'aide de la CLI de Deadline Cloud, utilisez la commande suivante pour définir le paramètre `storage-profile-id` de configuration :

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

Nombre maximum de tâches ayant échoué

L'`max-failed-tasks-count`option définit le nombre maximum de tâches susceptibles d'échouer avant que l'ensemble de la tâche échoue et que toutes les tâches restantes ne soient marquées`CANCELED`. La valeur par défaut est 100.

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

Nombre maximum de tentatives de tâches infructueuses

L'`max-retries-per-task`option définit le nombre maximal de fois qu'une tâche est réessayée avant qu'elle n'échoue. Lorsqu'une tâche est réessayée, elle est mise en `READY` état. La valeur par défaut est 5.

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

Planification des tâches dans Deadline Cloud

Après la création d'une tâche, AWS Deadline Cloud planifie son traitement sur une ou plusieurs flottes associées à une file d'attente. La flotte qui traite une tâche particulière est choisie en fonction des capacités configurées pour la flotte et des exigences de l'hôte pour une étape spécifique.

Les tâches sont planifiées dans l'ordre de priorité du meilleur effort, du plus haut au plus bas. Lorsque deux tâches ont la même priorité, la tâche la plus ancienne est planifiée en premier.

Les sections suivantes fournissent des informations détaillées sur le processus de planification d'une tâche.

Déterminer la compatibilité de la flotte

Après la création d'une tâche, Deadline Cloud vérifie les exigences de l'hôte pour chaque étape de la tâche par rapport aux capacités des flottes associées à la file d'attente à laquelle la tâche a été soumise. Si une flotte répond aux exigences de l'hôte, le poste est confié à l'`READY`État.

Si une étape de la tâche comporte des exigences qui ne peuvent pas être satisfaites par une flotte associée à la file d'attente, le statut de l'étape est défini sur`NOT_COMPATIBLE`. De plus, les autres étapes de la tâche sont annulées.

Les capacités d'une flotte sont définies au niveau de la flotte. Même si un travailleur d'un parc répond aux exigences du poste, aucune tâche ne lui sera affectée si son parc ne répond pas aux exigences du poste.

Le modèle de tâche suivant comporte une étape qui spécifie les exigences de l'hôte pour l'étape :

```
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
```

Cette tâche peut être planifiée pour une flotte dotée des fonctionnalités suivantes :

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

Cette tâche ne peut pas être planifiée pour une flotte dotée de l'une des fonctionnalités suivantes :

```
{
    "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.
```

Dimensionnement du parc

Lorsqu'une tâche est attribuée à un parc géré par des services compatibles, le parc est redimensionné automatiquement. Le nombre de travailleurs de la flotte fluctue en fonction du nombre de tâches pouvant être exécutées par la flotte.

Lorsqu'une tâche est attribuée à un parc géré par le client, il se peut que des travailleurs existent déjà ou qu'ils puissent être créés à l'aide de l'autoscaling basé sur les événements. Pour plus d'informations, consultez la section Utiliser EventBridge pour gérer les événements de dimensionnement automatique dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Séances

Les tâches d'une tâche sont divisées en une ou plusieurs sessions. Les travailleurs exécutent les sessions pour configurer l'environnement, exécuter les tâches, puis détruire l'environnement. Chaque session est composée d'une ou de plusieurs actions que le travailleur doit effectuer.

Au fur et à mesure qu'un collaborateur exécute des actions de section, des actions de session supplémentaires peuvent lui être envoyées. Le travailleur réutilise les environnements existants et les pièces jointes aux tâches au cours de la session pour effectuer les tâches de manière plus efficace.

Les pièces jointes aux tâches sont créées par l'émetteur que vous utilisez, dans le cadre de votre offre de tâches Deadline Cloud CLI. Vous pouvez également créer des pièces jointes à des tâches en utilisant l'`--attachments`option de `create-job` AWS CLI commande. Les environnements sont définis à deux endroits : les environnements de file d'attente attachés à une file d'attente spécifique et les environnements d'étapes de travail définis dans le modèle de travail.

Il existe quatre types d'actions de session :

- `syncInputJobAttachments`— Télécharge les pièces jointes aux tâches saisies vers le travailleur.
- `envEnter`— Exécute les `onEnter` actions pour un environnement.
- `taskRun`— Exécute les onRun actions d'une tâche.
- `envExit`— Exécute les `onExit` actions pour un environnement.

Le modèle de tâche suivant comporte un environnement par étapes. Il contient une `onEnter` définition pour configurer l'environnement des étapes, une onRun définition qui définit la tâche à exécuter et une `onExit` définition pour démonter l'environnement des étapes. Les sessions créées pour cette tâche incluront une `envEnter` action, une ou plusieurs `taskRun` actions, puis une `envExit` action.

```
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 }}
```

Dépendances des étapes

Deadline Cloud prend en charge la définition des dépendances entre les étapes afin qu'une étape attende la fin d'une autre étape avant de commencer. Vous pouvez définir plusieurs interdépendances pour une étape. Une étape comportant une dépendance n'est planifiée que lorsque toutes ses dépendances sont terminées.

Si le modèle de tâche définit une dépendance circulaire, la tâche est rejetée et son statut est défini sur`CREATE_FAILED`.

Le modèle de tâche suivant crée une tâche en deux étapes. `StepB`dépend de`StepA`. `StepB`ne s'exécute qu'une fois `StepA` terminé avec succès.

Une fois le travail créé, `StepA` il est dans l'`READY`état et `StepB` est dans l'`PENDING`état. Après avoir `StepA` terminé, `StepB` passe à l'`READY`état. En cas d'`StepA`échec ou `StepA` d'annulation, `StepB` passe à l'`CANCELED`état.

Vous pouvez définir une dépendance pour plusieurs étapes. Par exemple, si `StepC` cela dépend des deux `StepA` et`StepB`, `StepC` ne démarrera pas tant que les deux autres étapes ne seront pas terminées.

```
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!
```

États des tâches dans la CLI de Deadline Cloud

Cette rubrique décrit comment utiliser l'interface de ligne de commande de AWS Deadline Cloud (CLI de Deadline Cloud) pour afficher le statut d'une tâche ou d'une étape. Si vous souhaitez utiliser le moniteur Deadline Cloud pour consulter le statut des tâches ou des étapes, consultezAfficher et gérer les tâches, les étapes et les tâches dans Deadline Cloud.

Vous pouvez consulter l'état d'une tâche à l'aide de la commande `deadline job get --job-id` Deadline Cloud CLI. La réponse aux commandes inclut le statut de la tâche ou de l'étape et le nombre de tâches dans chaque état de traitement.

Lorsque vous soumettez une offre d'emploi pour la première fois, le statut est`CREATE_IN_PROGRESS`. Si la tâche passe les contrôles de validation, son statut passe à`CREATE_COMPLETE`. Dans le cas contraire, le statut passe à`CREATE_FAILED`.

Parmi les raisons possibles pour lesquelles une tâche peut échouer aux contrôles de validation, citons les suivantes :

- Le modèle de tâche ne respecte pas la spécification OpenJD.
- La tâche contient trop d'étapes.
- La tâche contient un trop grand nombre de tâches au total.

Pour voir les quotas correspondant au nombre maximal d'étapes et de tâches d'une tâche, utilisez la console Service Quotas. Pour plus d'informations, consultez Quotas pour Deadline Cloud.

Il se peut également qu'une erreur de service interne empêche la création d'un emploi. Dans ce cas, le code d'état de la tâche est défini `INTERNAL_ERROR` et le champ du message d'état fournit une explication plus détaillée.

Utilisez la commande Deadline Cloud CLI suivante pour afficher les détails d'une tâche. Dans l'exemple suivant, remplacez *`jobID`*par vos propres informations :

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

La réponse de la `deadline job get` commande est la suivante :

```
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
```

Chaque tâche d'une tâche ou d'une étape possède un statut. Les statuts des tâches sont combinés pour donner un statut global aux tâches et aux étapes. Le nombre de tâches dans chaque état est indiqué dans le `taskRunStatusCounts` champ de la réponse.

Le statut d'une tâche ou d'une étape dépend de l'état de ses tâches. Le statut est déterminé par les tâches dotées de ces statuts, dans l'ordre. Les statuts des étapes sont déterminés de la même manière que le statut des tâches.

La liste suivante décrit les statuts :

`NOT_COMPATIBLE`

Le travail n'est pas compatible avec la ferme car aucune flotte ne peut effectuer l'une des tâches du travail.

`RUNNING`

Un ou plusieurs collaborateurs exécutent des tâches depuis le poste. Tant qu'au moins une tâche est en cours d'exécution, la tâche est marquée`RUNNING`.

`ASSIGNED`

Un ou plusieurs travailleurs se voient attribuer des tâches dans le cadre de leur tâche lors de leur prochaine action. L'environnement, le cas échéant, est configuré.

`STARTING`

Un ou plusieurs collaborateurs sont en train de configurer l'environnement pour exécuter les tâches.

`SCHEDULED`

Les tâches associées à la tâche sont planifiées pour un ou plusieurs travailleurs en tant que prochaine action du travailleur.

`READY`

Au moins une tâche correspondant à la tâche est prête à être traitée.

`INTERRUPTING`

Au moins une tâche du travail est interrompue. Des interruptions peuvent se produire lorsque vous mettez à jour manuellement le statut de la tâche. Cela peut également se produire en réponse à une interruption due aux variations de prix d'Amazon Elastic Compute Cloud (Amazon EC2) Spot.

`FAILED`

Une ou plusieurs tâches de la tâche n'ont pas été exécutées correctement.

`CANCELED`

Une ou plusieurs tâches de la tâche ont été annulées.

`SUSPENDED`

Au moins une tâche de la tâche a été suspendue.

`PENDING`

Une tâche en cours d'exécution est en attente de la disponibilité d'une autre ressource.

`SUCCEEDED`

Toutes les tâches du projet ont été traitées avec succès.

Modifier des tâches dans Deadline Cloud

Vous pouvez utiliser les `update` commandes suivantes AWS Command Line Interface (AWS CLI) pour modifier la configuration d'une tâche ou pour définir le statut cible d'une tâche, d'une étape ou d'une tâche :

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

Dans les exemples de `update` commandes suivants, remplacez chacune *`user input placeholder`*par vos propres informations.

Vous pouvez également utiliser le moniteur Deadline Cloud pour modifier la configuration d'une tâche. Pour plus d'informations, consultez Afficher et gérer les tâches, les étapes et les tâches dans Deadline Cloud.

Example — Demander une offre d'emploi

Toutes les tâches de la tâche passent au `READY` statut, sauf s'il existe des dépendances entre les étapes. Les étapes comportant des dépendances passent à l'une `READY` ou l'autre à `PENDING` mesure qu'elles sont restaurées.

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

Example — Annuler une offre d'emploi

Toutes les tâches de la tâche qui n'ont pas le statut requis `SUCCEEDED` ou qui `FAILED` sont marquéesCANCELED.

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

Example — Marquer l'échec d'une tâche

Toutes les tâches du poste dont le statut est défini SUCCEEDED restent inchangées. Toutes les autres tâches sont marquéesFAILED.

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

Example — Marquer un travail réussi

Toutes les tâches du poste sont transférées à l'SUCCEEDEDétat.

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

Example — Suspendre une tâche

Les tâches du poste dans l'FAILEDétat SUCCEEDEDCANCELED, ou ne changent pas. Toutes les autres tâches sont marquéesSUSPENDED.

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

Example — Modifier la priorité d'une tâche

Met à jour la priorité d'une tâche pour modifier l'ordre dans lequel elle est planifiée. Les tâches les plus prioritaires sont généralement planifiées en premier.

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

Example — Modifie le nombre de tâches échouées autorisées

Actualise le nombre maximum de tâches échouées que la tâche peut avoir avant que les tâches restantes ne soient annulées.

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

Example — Modifie le nombre de tentatives de tâches autorisées

Actualise le nombre maximal de tentatives pour une tâche avant que celle-ci n'échoue. Une tâche ayant atteint le nombre maximum de tentatives ne peut pas être mise en attente tant que cette valeur n'est pas augmentée.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--max-retries-per-task 10
```

Example — Archiver une tâche

Met à jour l'état du cycle de vie de la tâche surARCHIVED. Les tâches archivées ne peuvent être ni planifiées ni modifiées. Vous ne pouvez archiver qu'une tâche dont l'SUSPENDEDétat est FAILED CANCELEDSUCCEEDED,, ou.

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

Example — Demander une étape

Toutes les tâches de l'étape passent à l'READYétat, sauf s'il existe des dépendances entre les étapes. Les tâches des étapes comportant des dépendances passent à l'une READY ou l'autrePENDING, et la tâche est restaurée.

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

Example — Annuler une étape

Toutes les tâches de l'étape qui n'ont pas le statut `SUCCEEDED` ou qui `FAILED` sont marquées`CANCELED`.

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

Example — Marquer l'échec d'une étape

Toutes les tâches de l'étape dont le statut est `SUCCEEDED` défini restent inchangées. Toutes les autres tâches sont marquées`FAILED`.

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

Example — Marquer une étape comme réussie

Toutes les tâches de l'étape sont marquées`SUCCEEDED`.

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

Example — Suspendre une étape

Les tâches de l'étape à l'`FAILED`état `SUCCEEDED``CANCELED`, ou ne changent pas. Toutes les autres tâches sont marquées`SUSPENDED`.

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

Example — Modifier le statut d'une tâche

Lorsque vous utilisez la commande `update-task` Deadline Cloud CLI, la tâche passe à l'état spécifié.

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

Comment Deadline Cloud traite les tâches

Pour traiter une tâche, AWS Deadline Cloud utilise le modèle de tâche Open Job Description (OpenJD) pour déterminer les ressources nécessaires. Deadline Cloud sélectionne un travailleur approprié pour une étape parmi les flottes associées à votre file d'attente. Le travailleur sélectionné possède tous les attributs de capacité requis pour l'étape.

Deadline Cloud envoie ensuite des instructions aux travailleurs pour qu'ils configurent une session pour l'étape. Le logiciel requis pour l'étape doit être disponible sur l'instance de travail pour que la tâche puisse s'exécuter. Le service peut ouvrir des sessions sur plusieurs travailleurs si les paramètres de dimensionnement de la flotte ont une capacité suffisante.

Vous pouvez configurer le logiciel dans un Amazon Machine Image (AMI), ou votre utilisateur peut le charger au moment de l'exécution à partir d'un référentiel ou d'un gestionnaire de packages. Vous

pouvez utiliser des environnements de file d'attente, de tâche ou d'étapes pour déployer le logiciel que vous préférez.

Le service Deadline Cloud utilise le modèle OpenJD pour déterminer les étapes requises pour la tâche et les tâches requises pour chaque étape. Certaines étapes sont dépendantes d'autres étapes, c'est pourquoi Deadline Cloud détermine l'ordre dans lequel les étapes doivent être effectuées. Deadline Cloud envoie ensuite les tâches correspondant à chaque étape aux collaborateurs pour qu'ils les traitent. Lorsqu'une tâche est terminée, le service envoie une autre tâche au cours de la même session, ou le travailleur peut démarrer une nouvelle session.

Vous pouvez suivre la progression de la tâche dans le moniteur Deadline Cloud, l'interface de ligne de commande de Deadline Cloud (CLI Deadline Cloud) ou le AWS CLI. Pour plus d'informations sur l'utilisation du moniteur, consultezUtilisation du moniteur Deadline Cloud. Pour plus d'informations sur l'utilisation de la CLI Deadline Cloud, consultezÉtats des tâches dans la CLI de Deadline Cloud.

Une fois toutes les tâches de chaque étape terminées, le travail est terminé et le résultat est prêt à être téléchargé sur votre poste de travail. Même si le travail n'est pas terminé, le résultat de chaque étape et tâche terminée peut être téléchargé.

Deadline Cloud supprime les offres d'emploi 120 jours après leur soumission. Lorsqu'une tâche est supprimée, toutes les étapes et tâches associées à la tâche sont également supprimées. Si vous devez réexécuter la tâche, soumettez à nouveau le modèle OpenJD correspondant à la tâche.

Résolution des problèmes liés à Deadline Cloud

Pour plus d'informations sur les problèmes courants liés aux tâches dans AWS Deadline Cloud, consultez les rubriques suivantes.

Rubriques

- Pourquoi la création de mon emploi a-t-elle échoué ?
- Pourquoi mon travail n'est-il pas compatible ?
- Pourquoi mon travail est-il prêt ?
- Pourquoi mon travail a-t-il échoué ?
- Pourquoi mon étape est-elle en attente ?

Pourquoi la création de mon emploi a-t-elle échoué ?

Parmi les raisons possibles pour lesquelles une tâche peut échouer aux contrôles de validation, citons les suivantes :

- Le modèle de tâche ne respecte pas la spécification OpenJD.
- La tâche contient trop d'étapes.
- La tâche contient un trop grand nombre de tâches au total.
- Une erreur de service interne a empêché la création de la tâche.

Pour voir les quotas correspondant au nombre maximal d'étapes et de tâches d'une tâche, utilisez la console Service Quotas. Pour plus d'informations, consultez Quotas pour Deadline Cloud.

Pourquoi mon travail n'est-il pas compatible ?

Les raisons courantes pour lesquelles les tâches ne sont pas compatibles avec les files d'attente sont les suivantes :

- Aucune flotte n'est associée à la file d'attente à laquelle le travail a été soumis. Ouvrez le moniteur Deadline Cloud et vérifiez que des flottes sont associées à la file d'attente. Pour plus d'informations sur l'affichage des files d'attente, consultezAfficher les détails de la file d'attente et de la flotte dans Deadline Cloud.
- La tâche comporte des exigences en matière d'hôte qui ne sont satisfaites par aucune des flottes associées à la file d'attente. Pour vérifier, comparez l'`hostRequirements`entrée dans le modèle de tâche avec la configuration des flottes de votre ferme. Assurez-vous que l'une des flottes répond aux exigences de l'hôte. Pour plus d'informations sur la compatibilité des flottes, consultezDéterminer la compatibilité de la flotte. Pour consulter la configuration du parc, voirAfficher les détails de la file d'attente et de la flotte dans Deadline Cloud.

Pourquoi mon travail est-il prêt ?

Les raisons possibles pour lesquelles votre emploi semble bloqué dans l'`READY`État sont les suivantes :

- Le nombre maximum de travailleurs pour les flottes associées à la file d'attente est fixé à zéro. Pour vérifier, consultezAfficher les détails de la file d'attente et de la flotte dans Deadline Cloud.

- Il y a une tâche plus prioritaire dans la file d'attente. Pour vérifier, consultezAfficher les détails de la file d'attente et de la flotte dans Deadline Cloud.
- Pour les flottes gérées par le client, vérifiez la configuration de mise à l'échelle automatique. Pour plus d'informations, consultez Faites évoluer automatiquement votre flotte Amazon EC2 grâce à la fonction de recommandation de dimensionnement de Deadline Cloud.

Pourquoi mon travail a-t-il échoué ?

Un travail peut échouer pour de nombreuses raisons. Pour rechercher le problème, ouvrez le moniteur Deadline Cloud et choisissez la tâche défaillante. Choisissez une tâche qui a échoué, puis consultez les journaux de cette tâche. Pour obtenir des instructions, veuillez consulter Afficher les journaux dans Deadline Cloud.

- Si vous constatez des erreurs de licence ou si un filigrane apparaît parce que le logiciel ne possède pas de licence valide, assurez-vous que le travailleur peut se connecter au serveur de licences requis. Pour plus d'informations, consultez Connectez les flottes gérées par le client à un point de terminaison de licence.

Pourquoi mon étape est-elle en attente ?

Les étapes peuvent rester dans `PENDING` cet état lorsqu'une ou plusieurs de leurs dépendances ne sont pas complètes. Vous pouvez vérifier l'état des dépendances à l'aide du moniteur Deadline Cloud. Pour obtenir des instructions, veuillez consulter Afficher une étape dans Deadline Cloud.

Stockage de fichiers pour Deadline Cloud

Les travailleurs doivent avoir accès aux emplacements de stockage qui contiennent les fichiers d'entrée nécessaires au traitement d'une tâche, ainsi qu'aux emplacements qui stockent la sortie. AWS Deadline Cloud propose deux options pour les emplacements de stockage :

- Avec les pièces jointes aux tâches, Deadline Cloud transfère les fichiers d'entrée et de sortie de vos tâches dans les deux sens entre un poste de travail et les collaborateurs de Deadline Cloud. Pour activer les transferts de fichiers, Deadline Cloud utilise un bucket Amazon Simple Storage Service (Amazon S3) dans votre. Compte AWS

  Lorsque vous utilisez des pièces jointes à des tâches avec un parc géré par des services, vous pouvez configurer un système de fichiers virtuel (VFS) dans votre réseau privé virtuel (VPN). Les travailleurs peuvent alors charger des fichiers uniquement lorsque cela est nécessaire.
- Avec le stockage partagé, vous utilisez le partage de fichiers avec votre système d'exploitation pour permettre l'accès aux fichiers.

  Lorsque vous utilisez le stockage partagé multiplateforme, vous pouvez créer un profil de stockage afin que les utilisateurs puissent mapper le chemin d'accès aux fichiers entre deux systèmes d'exploitation différents.

Rubriques

Pièces jointes aux offres d'emploi dans Deadline Cloud

Les pièces jointes aux tâches vous permettent de transférer des fichiers entre votre poste de travail et AWS Deadline Cloud. Avec les pièces jointes aux tâches, vous n'avez pas besoin de configurer manuellement un compartiment Amazon S3 pour vos fichiers. Au lieu de cela, lorsque vous créez une file d'attente avec la console Deadline Cloud, vous choisissez le bucket pour les pièces jointes à vos tâches.

La première fois que vous soumettez une tâche à Deadline Cloud, tous les fichiers de la tâche sont transférés vers Deadline Cloud. Pour les soumissions ultérieures, seuls les fichiers modifiés sont transférés, ce qui permet d'économiser du temps et de la bande passante.

Une fois le traitement terminé, vous pouvez télécharger le résultat depuis la page détaillée de la tâche ou à l'aide de la `deadline job download-output` commande Deadline Cloud CLI.

Vous pouvez utiliser le même compartiment S3 pour plusieurs files d'attente. Définissez un préfixe racine différent pour chaque file d'attente afin d'organiser les pièces jointes dans le compartiment.

Lorsque vous créez une file d'attente avec la console, vous pouvez choisir un rôle AWS Identity and Access Management (IAM) existant ou demander à la console de créer un nouveau rôle. Si la console crée le rôle, elle définit les autorisations d'accès au compartiment spécifié pour la file d'attente. Si vous choisissez un rôle existant, vous devez lui accorder les autorisations d'accès au compartiment S3.

Chiffrement pour les compartiments S3 associés aux tâches

Les fichiers joints aux tâches sont automatiquement chiffrés dans votre compartiment S3 par défaut. Cette approche permet de protéger vos informations contre tout accès non autorisé. Vous n'avez rien à faire pour que vos fichiers soient chiffrés à l'aide des clés fournies par Deadline Cloud. Pour plus d'informations, consultez le guide de l'utilisateur Amazon S3 qui chiffre désormais automatiquement tous les nouveaux objets.

Vous pouvez utiliser votre propre AWS Key Management Service clé gérée par le client pour chiffrer le compartiment S3 qui contient les pièces jointes à vos tâches. Pour ce faire, vous devez modifier le rôle IAM de la file d'attente associée au bucket afin de permettre l'accès au AWS KMS key.

Pour ouvrir l'éditeur de stratégie IAM pour le rôle de file d'attente

1. Connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la. Sur la page principale, dans la section Commencer, choisissez Afficher les fermes.
2. Dans la liste des parcs de serveurs, choisissez le parc contenant la file d'attente à modifier.
3. Dans la liste des files d'attente, choisissez la file à modifier.
4. Dans la section Détails de la file d'attente, choisissez le rôle de service pour ouvrir la console IAM correspondant au rôle de service.

Effectuez ensuite la procédure suivante.

Pour mettre à jour la politique de rôle avec l'autorisation de AWS KMS

1. Dans la liste des politiques d'autorisations, choisissez la politique du rôle.
2. Dans la section Autorisations définies dans cette politique, choisissez Modifier.

3. Choisissez Ajouter un nouveau relevé.
4. Copiez et collez la politique suivante dans l'éditeur. Changez le *RegionaccountID*, et *keyID*selon vos propres valeurs.

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

5. Choisissez Suivant.
6. Passez en revue les modifications apportées à la politique, puis lorsque vous êtes satisfait, choisissez Enregistrer les modifications.

Gestion des pièces jointes aux tâches dans les compartiments S3

Deadline Cloud stocke les fichiers joints requis pour votre tâche dans un compartiment S3. Ces fichiers s'accumulent au fil du temps, ce qui augmente les coûts d'Amazon S3. Pour réduire les coûts, vous pouvez appliquer une configuration S3 Lifecycle à votre compartiment S3. Cette configuration permet de supprimer automatiquement les fichiers du compartiment. Comme le compartiment S3 se trouve dans votre compte, vous pouvez choisir de modifier ou de supprimer la configuration du cycle de vie S3 à tout moment. Pour plus d'informations, consultez la section Exemples de configuration du cycle de vie S3 dans le guide de l'utilisateur Amazon S3.

Pour une solution de gestion des compartiments S3 plus précise, vous pouvez configurer vos objets Compte AWS pour qu'ils expirent dans un compartiment S3 en fonction de leur dernier accès. Pour plus d'informations, consultez la section Expiration des objets Amazon S3 en fonction de la date du dernier accès afin de réduire les coûts sur le blog AWS d'architecture.

Système de fichiers virtuel Deadline Cloud

La prise en charge du système de fichiers virtuel pour les pièces jointes aux tâches dans AWS Deadline Cloud permet au logiciel client sur les employés de communiquer directement avec Amazon

Simple Storage Service. Les travailleurs peuvent charger des fichiers uniquement lorsque cela est nécessaire au lieu de télécharger tous les fichiers avant le traitement. Les fichiers sont stockés localement. Cette approche permet d'éviter de télécharger des ressources utilisées plusieurs fois. Tous les fichiers sont supprimés une fois le travail terminé.

- Le système de fichiers virtuel améliore considérablement les performances pour des profils de travail spécifiques. En général, ce sont les petits sous-ensembles du nombre total de fichiers comportant des flottes de travailleurs plus importantes qui présentent le plus d'avantages. Les délais de traitement sont à peu près équivalents pour un petit nombre de dossiers nécessitant moins de personnel.
- La prise en charge des systèmes de fichiers virtuels n'est disponible que pour Linux les employés des flottes gérées par des services.
- Le système de fichiers virtuel Deadline Cloud prend en charge les opérations suivantes, mais n'est pas compatible avec POSIX :
  - Fichier`create`,`delete`,`open`,`close`,`read`,`write`,`append`,`truncate`,`rename`,`move`,`copy`,`stat`,`fsyn` et `falloc`
  - Répertoire`create`, `delete``rename`,`move`,`copy`, et `stat`
- Le système de fichiers virtuel est conçu pour réduire le transfert de données et améliorer les performances lorsque vos tâches n'accèdent qu'à une partie d'un ensemble de données volumineux. Il n'est pas optimisé pour toutes les charges de travail. Vous devez tester votre charge de travail avant d'exécuter des tâches de production.

Activer le support VFS

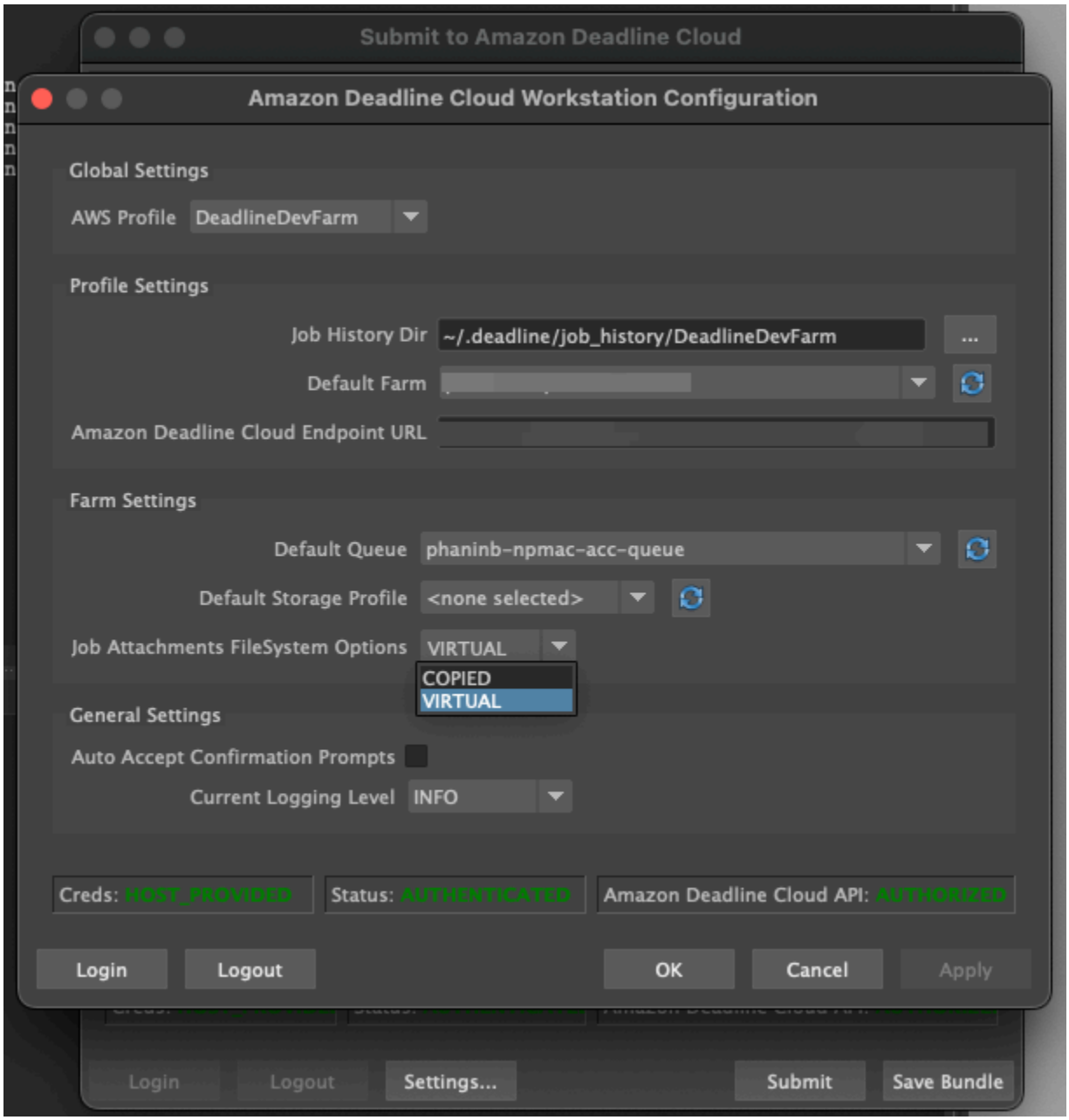
Le support du système de fichiers virtuel (VFS) est activé pour chaque tâche. Une tâche revient au cadre de pièces jointes par défaut dans les cas suivants :

- Un profil d'instance de travail ne prend pas en charge un système de fichiers virtuel.
- Des problèmes empêchent le lancement du processus du système de fichiers virtuel.
- Le système de fichiers virtuel ne peut pas être monté.

Pour activer la prise en charge du système de fichiers virtuel à l'aide de l'expéditeur

1. Lorsque vous soumettez une tâche, cliquez sur le bouton Paramètres pour ouvrir le panneau de configuration du poste de travail AWS Deadline Cloud.

2. Dans le menu déroulant des options du système de fichiers Job attachments, sélectionnez VIRTUAL.



3. Pour enregistrer vos modifications, cliquez sur OK.

Pour activer la prise en charge des systèmes de fichiers virtuels à l'aide du AWS CLI

- Utilisez la commande suivante lorsque vous soumettez une tâche enregistrée :

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

Pour vérifier que le système de fichiers virtuel a été lancé correctement pour une tâche donnée, consultez vos journaux dans Amazon CloudWatch Logs. Recherchez les messages suivants :

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

Si le journal contient le message suivant, le support du système de fichiers virtuel est désactivé :

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

Résolution des problèmes liés au support des systèmes de fichiers virtuels

Vous pouvez consulter les journaux de votre système de fichiers virtuel à l'aide du moniteur Deadline Cloud. Pour obtenir des instructions, veuillez consulter Afficher les journaux dans Deadline Cloud.

Les journaux du système de fichiers virtuel sont également envoyés au groupe CloudWatch Logs associé à la file d'attente partagée avec la sortie de l'agent de travail.

Stockage partagé dans Deadline Cloud

Pour utiliser le stockage partagé, les collaborateurs utilisent le système de partage de fichiers du système d'exploitation pour accéder à un espace de stockage partagé pour l'entrée et la sortie de vos tâches.

La méthode que vous utilisez pour partager des fichiers dépend de votre système d'exploitation et de la manière dont vous implémentez le stockage partagé sur votre réseau. Vous êtes responsable de la manière dont vous configurez le partage de fichiers et de vous assurer qu'il répond à vos besoins.

Si vous utilisez une solution de partage de fichiers entre systèmes, vous pouvez utiliser des profils de stockage pour mapper les emplacements des fichiers entre Linux les systèmes de Windows fichiers.

Profils de stockage dans Deadline Cloud

Un profil de stockage vous permet de configurer des fermes à l'aide d'un stockage partagé multiplateforme. Un profil de stockage trace les chemins entre les systèmes d'exploitation pour les tâches traitées par des employés utilisant un système d'exploitation différent de celui du poste de travail à partir duquel ils ont été soumis.

Les profils de stockage sont nécessaires lorsque vous utilisez un parc géré par le client avec une combinaison de systèmes d'exploitation utilisés par des postes de travail et des employés. Les profils de stockage ne sont pas pris en charge sur les flottes gérées par des services.

Après avoir créé un profil de stockage, vous devez autoriser l'accès aux files d'attente et aux flottes qui utilisent le profil.

Pour créer un profil de stockage

1. Ouvrez la console Deadline Cloud.
2. Dans Commencer, choisissez Accéder au tableau de bord de Deadline Cloud.
3. Choisissez un parc de serveurs, puis cliquez sur l'onglet Profils de stockage.
4. Choisissez Créer un profil de stockage.
5. Choisissez un système d'exploitation dans le menu déroulant.
6. Entrez un nom pour le profil. Un nom clair vous permet de choisir le profil de stockage à utiliser lors de la soumission de tâches.
7. Pour le nom du chemin, entrez l'emplacement racine des données de travail sur le poste de travail à partir duquel vous soumettez des tâches.
8. Choisissez un type de stockage :
   - Local fait référence aux emplacements de fichiers qui ne sont pas partagés entre le travailleur et le poste de travail. Elles sont téléchargées sous forme de pièces jointes aux offres d'emploi.
   - Le partage fait référence au stockage partagé entre le travailleur et le poste de travail. Les fichiers stockés dans le stockage partagé ne sont pas chargés sous forme de pièces jointes à des tâches.
9. Indiquez le chemin d'emplacement du système de fichiers. Il s'agit du répertoire racine de vos données de travail.
10. Choisissez Créer.

Après avoir créé un profil de stockage, vous devez modifier vos files d'attente et vos flottes gérées par les clients pour utiliser le nouveau profil. Pour autoriser l'accès à un profil de stockage, appliquez la procédure suivante une fois que vous avez terminé la procédure précédente.

Pour autoriser les files d'attente et les flottes gérées par les clients à utiliser un profil de stockage

1. Choisissez l'onglet Files d'attente ou Fleets.

2. Choisissez la file d'attente ou le parc à modifier.
3. Choisissez Modifier les profils de stockage.
4. Sélectionnez le profil de stockage à autoriser, ainsi que les emplacements du système de fichiers à partir de ce profil.
5. Sélectionnez Enregistrer les modifications.

Gestion des budgets et de l'utilisation pour Deadline Cloud

Le gestionnaire de budget et l'explorateur d'utilisation de AWS Deadline Cloud sont des outils de gestion des coûts qui fournissent le coût approximatif de l'utilisation de Deadline Cloud sur la base des informations disponibles sur les variables de coût. Les outils de gestion des coûts ne garantissent pas le montant dû pour votre utilisation réelle de Deadline Cloud et d'autres AWS services.

Pour vous aider à gérer les coûts de Deadline Cloud, vous pouvez utiliser les fonctionnalités suivantes :

- Gestionnaire de budget — Avec le gestionnaire de budget de Deadline Cloud, vous pouvez créer et modifier des budgets pour mieux gérer les coûts des projets.
- Explorateur d'utilisation : avec l'explorateur d'utilisation de Deadline Cloud, vous pouvez consulter le nombre de AWS ressources utilisées et les coûts estimés de ces ressources.

Hypothèses de coûts

Le calcul de base utilisé par les outils de gestion des coûts de Deadline Cloud est le suivant :

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

- Le temps d'exécution est la somme de toutes les tâches d'une tâche, de l'heure de début à l'heure de fin.
- Le taux de calcul est déterminé par la tarification de AWS Deadline Cloud pour les flottes gérées par des services. Pour les flottes gérées par le client, le taux de calcul est estimé à 1 dollar par heure de travail.
- Le taux de licence est déterminé par le prix de la licence de base de Deadline Cloud. Les niveaux supplémentaires ne sont pas inclus. Pour plus d'informations sur la tarification des licences, consultez la section Tarification de AWS Deadline Cloud.

L'estimation des coûts établie par les outils de gestion des coûts de Deadline Cloud peut différer de vos coûts réels pour un certain nombre de raisons. Les raisons courantes incluent :

- Les ressources détenues par les clients et leur tarification. Vous pouvez choisir d'apporter vos propres ressources, qu'elles proviennent AWS ou non de fournisseurs sur site ou d'autres fournisseurs de cloud. Les coûts réels de ces ressources ne sont pas calculés.
- Coûts liés aux travailleurs inactifs. Pour les flottes dont le nombre minimum d'instances est supérieur à zéro, les travailleurs inactifs ne sont pas pris en compte dans les calculs.
- Crédits promotionnels, remises et accords de tarification personnalisés. Les outils de gestion des coûts ne tiennent pas compte des crédits promotionnels, des accords de prix privés ou des autres remises. Vous pouvez être éligible à d'autres remises qui ne font pas partie de l'estimation.
- Stockage des actifs. Le stockage des actifs n'est pas inclus dans les estimations de coûts et d'utilisation.
- Changements de prix. AWS propose des pay-as-you-go prix pour la plupart des services. Les prix peuvent changer au fil du temps. Les outils de gestion des coûts utilisent le plus grand nombre de up-to-date prix disponibles auprès du public, mais il peut y avoir des retards après les modifications.
- Impôts. Les outils de gestion des coûts n'incluent pas les taxes appliquées à notre achat du service.
- Arrondi. L'outil de gestion des coûts effectue un arrondissement mathématique des données de tarification.
- Devise. Les estimations de coûts sont établies en dollars américains. Les taux de change mondiaux varient au fil du temps. Si vous traduisez des estimations dans une devise différente sur le taux de change actuel, les variations du taux de change affectent l'estimation.
- Licences externes. Si vous choisissez d'utiliser des licences préachetées (apportez votre propre licence), les outils de gestion des coûts de Deadline Cloud ne peuvent pas prendre en compte ce coût.

Utiliser le gestionnaire de budget de Deadline Cloud

Le gestionnaire de budget de Deadline Cloud vous aide à contrôler les dépenses relatives à une ressource donnée, telle qu'une file d'attente, un parc ou un parc de véhicules. Vous pouvez créer des montants et des limites budgétaires, et définir des actions automatisées pour réduire ou arrêter les dépenses supplémentaires par rapport au budget.

Les sections suivantes décrivent les étapes à suivre pour utiliser le gestionnaire de budget de Deadline Cloud.

Rubriques

Prérequis

Pour utiliser le gestionnaire de budget de Deadline Cloud, vous devez disposer `OWNER` d'un niveau d'accès. Pour accorder une `OWNER` autorisation, suivez les étapes décrites dansGestion des utilisateurs dans Deadline Cloud.

Accédez au gestionnaire de budget

Pour accéder au gestionnaire de budget de Deadline Cloud, suivez la procédure ci-dessous.

1. Connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la.
2. Choisissez Afficher les fermes.
3. Localisez la ferme sur laquelle vous souhaitez obtenir des informations, puis choisissez Gérer les tâches. Le moniteur Deadline Cloud s'ouvre dans un nouvel onglet.
4. Dans le moniteur Deadline Cloud, dans le volet de navigation de gauche, sélectionnez Budgets.

La page récapitulative du gestionnaire de budget affiche une liste des budgets actifs et inactifs :

- Les budgets actifs sont suivis par rapport à la ressource sélectionnée (une file d'attente).
- Les budgets inactifs ont expiré ou ont été annulés par un utilisateur, et les coûts ne sont plus mesurés par rapport aux limites de ce budget.

Une fois que vous avez choisi un budget, la page de résumé du budget contient des informations de base sur le budget. Les informations fournies incluent le nom du budget, son statut, les ressources, le pourcentage restant, le montant restant, le budget total, les dates de début et de fin.

Création d'un budget

Pour créer un budget, suivez la procédure ci-dessous.

1. Si ce n'est pas déjà fait, connectez-vous au AWS Management Console, ouvrez la console Deadline Cloud, choisissez une ferme, puis choisissez Gérer les tâches.
2. Sur la page du gestionnaire de budget, choisissez Créer un budget.
3. Dans la section Détails, entrez un nom de budget pour le budget.
4. (Facultatif) Dans le champ de description, entrez une brève description claire du budget.
5. Dans Ressource, choisissez le menu déroulant File d'attente pour rechercher et sélectionner la file d'attente pour laquelle vous souhaitez créer un budget.
6. Pour Période, définissez les dates de début et de fin du budget en effectuant les étapes suivantes :

   a. Pour Date de début, entrez la première date du suivi du budget au format AAAA/MM/JJ, ou choisissez l'icône du calendrier et sélectionnez une date.

      La date de début par défaut est la date de création du budget.

   b. Pour Date de fin, entrez la dernière date du suivi du budget au format AAAA/MM/JJ ou cliquez sur l'icône du calendrier et sélectionnez une date.

      La date de fin par défaut est de 120 jours à compter de la date de début.
7. Dans Montant du budget, entrez le montant en dollars du budget.
8. (Facultatif) Nous vous recommandons de créer des alertes de limite. Dans la section Limiter les actions, vous pouvez implémenter des actions automatisées qui se produisent lorsque des montants spécifiques restent dans le budget. Pour y arriver, exécutez les étapes suivantes.

   a. Choisissez Ajouter une nouvelle action.

   b. Dans le champ Montant restant, entrez le montant en dollars que vous souhaitez lancer l'action.

   c. Dans le menu déroulant Action, sélectionnez l'action de votre choix. Les actions incluent :

      - Arrêter après avoir terminé le travail en cours — Tous les travaux en cours lorsque le montant seuil est atteint continuent de s'exécuter (et entraînent des coûts) jusqu'à leur fin.
      - Arrêter immédiatement le travail — Tous les travaux sont annulés immédiatement lorsque le seuil est atteint.

d. Pour créer des alertes de limite supplémentaires, choisissez Ajouter une nouvelle action et répétez les deux étapes précédentes.

9. Choisissez Créer un budget. La page du gestionnaire de budget apparaît. Le budget nouvellement créé s'affiche dans l'onglet Budgets actifs.

Afficher un budget

Après avoir créé un budget, vous pouvez le consulter sur la page du gestionnaire de budget. À partir de là, vous pouvez voir le montant total du budget et le coût global alloué au budget spécifique.

Pour consulter un budget, suivez la procédure ci-dessous.

1. Si ce n'est pas déjà fait, connectez-vous au AWS Management Console, ouvrez la console Deadline Cloud, choisissez une ferme, puis choisissez Gérer les tâches.
2. Choisissez Budgets dans le volet de navigation de gauche. La page Gestionnaire de budget s'affiche.
3. Pour consulter un budget actif, cliquez sur l'onglet Budgets actifs, puis choisissez le nom du budget que vous souhaitez consulter. La page des détails du budget apparaît.
4. Pour consulter les détails du budget d'un budget expiré, cliquez sur l'onglet Budgets inactifs. Choisissez ensuite le nom du budget que vous souhaitez consulter. La page des détails du budget apparaît.

Modifier un budget

Vous pouvez modifier n'importe quel budget actif. Pour modifier un budget actif, procédez comme suit.

1. Si ce n'est pas déjà fait, connectez-vous au AWS Management Console, ouvrez la console Deadline Cloud, choisissez une ferme, puis choisissez Gérer les tâches.
2. Sur la page Gestionnaire de budget, dans l'onglet Budgets actifs, cliquez sur le bouton à côté du budget que vous souhaitez modifier.
3. Dans le menu déroulant Actions situé dans le coin supérieur droit, sélectionnez Modifier le budget.
4. Apportez les modifications souhaitées, puis choisissez Mettre à jour le budget.

Désactiver un budget

Vous pouvez désactiver n'importe quel budget actif. La désactivation d'un budget fait passer son statut d'actif à inactif. Lorsqu'un budget est désactivé, il n'assure plus le suivi d'une ressource par rapport au montant de ce budget.

Pour désactiver un budget, procédez comme suit.

1. Si ce n'est pas déjà fait, connectez-vous au AWS Management Console, ouvrez la console Deadline Cloud, choisissez une ferme, puis choisissez Gérer les tâches.
2. Sur la page Gestionnaire de budgets, dans l'onglet Budgets actifs, cliquez sur le bouton à côté du budget que vous souhaitez désactiver.
3. Dans le menu déroulant Actions situé dans le coin supérieur droit, sélectionnez Désactiver le budget. Dans quelques instants, le budget sélectionné passera d'actif à inactif et passera de l'onglet Budgets actifs à l'onglet Budgets inactifs.

Utilisation de l'explorateur d'utilisation de Deadline Cloud

Grâce à l'explorateur d'utilisation de Deadline Cloud, vous pouvez consulter des statistiques en temps réel sur l'activité de chaque ferme. Vous pouvez examiner les coûts de la ferme en fonction de différentes variables, telles que la file d'attente, le travail, le produit de licence ou le type d'instance. Sélectionnez différentes périodes pour voir l'utilisation au cours d'une période donnée et observez les tendances d'utilisation au fil du temps. Vous pouvez également consulter une ventilation détaillée des points de données sélectionnés, ce qui permet d'examiner de plus près les indicateurs. L'utilisation peut être indiquée par heure (minutes et heures) ou par coût (en dollars américains).

Les sections suivantes décrivent les étapes à suivre pour accéder à l'explorateur d'utilisation de Deadline Cloud et l'utiliser.

Rubriques

Prérequis

Pour utiliser l'explorateur d'utilisation de Deadline Cloud, vous devez disposer de l'une des autorisations nécessaires `MANAGER` ou d'`OWNER`une ferme de serveurs. Pour plus d'informations, consultez Gérez les utilisateurs et les groupes pour les fermes, les files d'attente et les flottes.

Ouvrez l'explorateur d'utilisation

Pour ouvrir l'explorateur d'utilisation de Deadline Cloud, procédez comme suit.

1. Connectez-vous à la console Deadline Cloud AWS Management Console et ouvrez-la.
2. Pour voir toutes les fermes disponibles, choisissez Afficher les fermes.
3. Localisez la ferme sur laquelle vous souhaitez obtenir des informations, puis choisissez Gérer les tâches. Le moniteur Deadline Cloud s'ouvre dans un nouvel onglet.
4. Dans le moniteur Deadline Cloud, dans le menu de gauche, sélectionnez Explorateur d'utilisation.

Utiliser l'explorateur d'utilisation

Sur la page de l'explorateur d'utilisation, vous pouvez sélectionner des paramètres spécifiques dans lesquels les données peuvent être affichées. Par défaut, vous voyez l'utilisation totale dans le temps (heures et minutes) au cours des 7 derniers jours. Vous pouvez modifier ces paramètres, et les informations affichées changent de manière dynamique en fonction des réglages des paramètres.

Vous pouvez regrouper les résultats en fonction de la file d'attente, de la tâche, de l'utilisation du calcul, du type d'instance ou du produit de licence. Si vous choisissez un produit de licence, les coûts sont calculés pour des licences spécifiques. Pour tous les autres groupes, le temps est calculé en additionnant le temps nécessaire à l'exécution de chaque tâche.

L'explorateur d'utilisation renvoie uniquement 100 résultats en fonction des critères de filtre que vous avez définis. Les résultats sont répertoriés par ordre décroissant selon l'horodatage de la date de création. S'il y a plus de 100 résultats, un message d'erreur s'affiche. Vous pouvez affiner votre requête pour réduire le nombre de résultats :

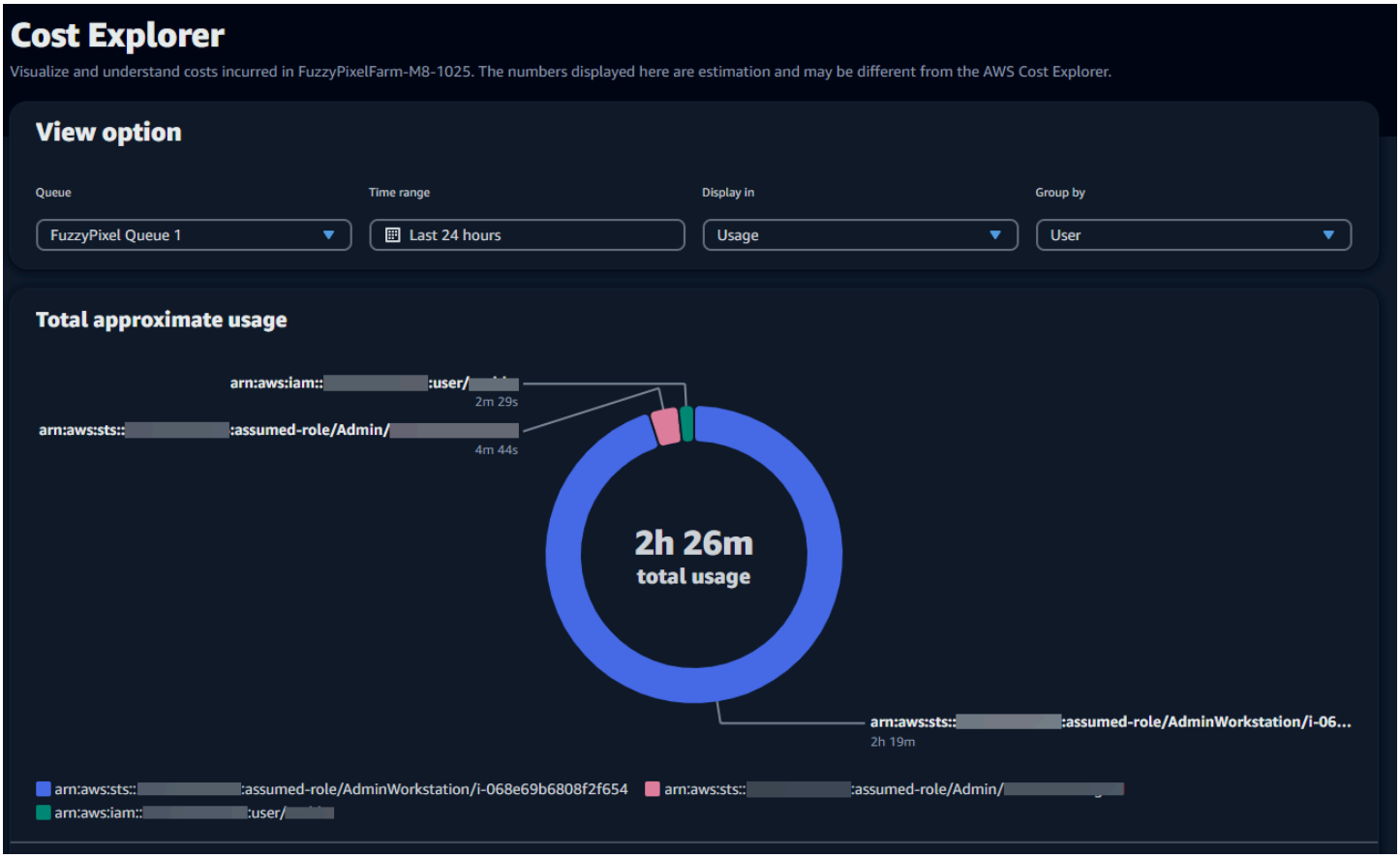
- Sélectionnez une plage de temps plus courte
- Sélectionnez moins de files d'attente
- Sélectionnez un autre regroupement, tel que le regroupement par file d'attente plutôt que par tâche

Rubriques

Utilisez des graphiques visuels pour examiner les données

Vous pouvez examiner les données dans un format visuel pour identifier les tendances et les domaines potentiels susceptibles de nécessiter une analyse ou une attention plus poussées. L'explorateur d'utilisation propose un graphique circulaire qui affiche l'utilisation globale et le coût avec la possibilité de regrouper les totaux en sous-totaux plus petits.

> **Note**
>
> Le graphique affiche uniquement les cinq premiers résultats, les autres résultats étant combinés dans une section « autres ». Vous pouvez consulter tous les résultats dans la section de répartition située sous le graphique.



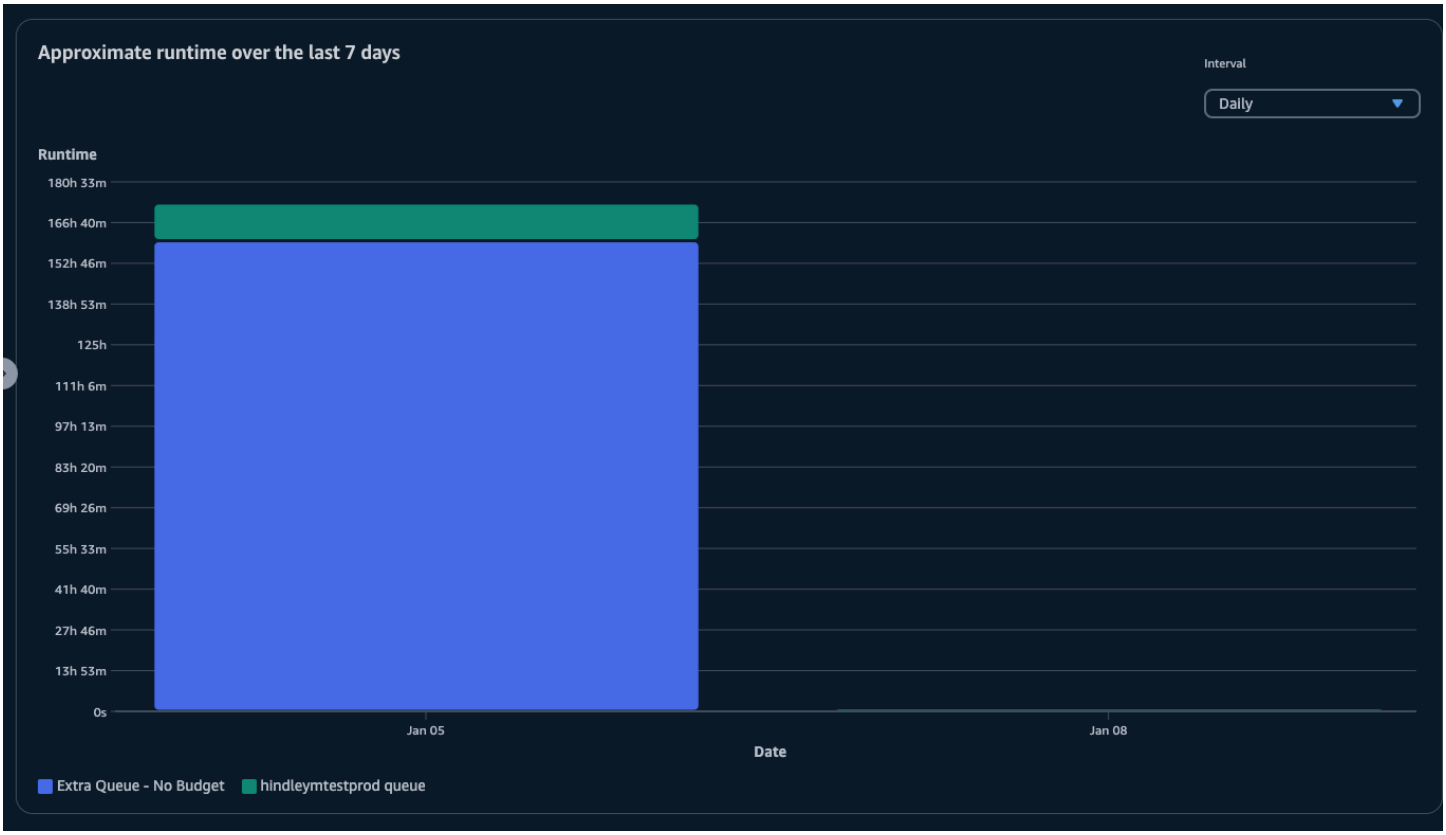
Afficher le détail des indicateurs

Sous le graphique circulaire, l'explorateur d'utilisation propose une ventilation plus détaillée de mesures spécifiques, qui changeront en fonction de l'évolution des paramètres. Par défaut, cinq résultats s'affichent dans l'explorateur d'utilisation. Vous pouvez faire défiler les résultats à l'aide des flèches de pagination dans la section de ventilation.

La panne est minimisée par défaut. Pour développer et afficher les résultats, sélectionnez la flèche de répartition Afficher tout. Pour télécharger le détail, choisissez Télécharger les données.

Afficher la durée approximative des files d'attente

Vous pouvez également afficher le temps d'exécution approximatif de vos files d'attente en fonction des différents intervalles que vous spécifiez. Les options d'intervalle sont les suivantes : horaire, quotidien, hebdomadaire et mensuel. Une fois que vous avez sélectionné un intervalle, le graphique affiche la durée approximative de vos files d'attente.



Gestion des coûts

AWS Deadline Cloud fournit des budgets et un explorateur d'utilisation pour vous aider à contrôler et à visualiser les coûts de vos tâches. Deadline Cloud utilise toutefois d'autres AWS services, tels qu'Amazon S3. Les coûts de ces services ne sont pas reflétés dans les budgets de Deadline Cloud ou dans l'explorateur d'utilisation et sont facturés séparément en fonction de l'utilisation. Selon la façon dont vous configurez Deadline Cloud, vous pouvez utiliser les AWS services suivants, ainsi que d'autres :

Service	Page de tarification
Amazon CloudWatch Logs	Tarification d'Amazon CloudWatch Logs
Amazon Elastic Compute Cloud	Tarification d'Amazon Elastic Compute Cloud
AWS Key Management Service	Tarification AWS Key Management Service
AWS PrivateLink	Tarification AWS PrivateLink

Service	Page de tarification
Amazon Simple Storage Service	Tarification Amazon S3
Amazon Virtual Private Cloud	Tarification d'Amazon Virtual Private Cloud

Bonnes pratiques en matière de gestion des coûts

L'utilisation des meilleures pratiques suivantes peut vous aider à comprendre et à contrôler vos coûts lorsque vous utilisez Deadline Cloud, ainsi que les compromis que vous pouvez faire entre coût et efficacité.

> **Note**
>
> Le coût final de l'utilisation de Deadline Cloud dépend de l'interaction entre un certain nombre de AWS services, de la quantité de travail que vous traitez et de l' Région AWS endroit où vous exécutez vos tâches. Les meilleures pratiques suivantes sont des directives et peuvent ne pas réduire les coûts de manière significative.

Bonnes pratiques pour les CloudWatch journaux

Deadline Cloud envoie les journaux des employés et des tâches à CloudWatch Logs. La collecte, le stockage et l'analyse de ces journaux vous sont facturés. Vous pouvez réduire les coûts en enregistrant uniquement le minimum de données nécessaires au suivi de vos tâches.

Lorsque vous créez une file d'attente ou un parc, Deadline Cloud crée un groupe de CloudWatch journaux Logs portant les noms suivants :

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

Par défaut, ces journaux n'expirent jamais. Vous pouvez ajuster la politique de conservation des groupes de journaux afin de supprimer les anciens journaux et de réduire les coûts de stockage. Vous pouvez également exporter des journaux vers Amazon S3. Les coûts de stockage d'Amazon S3 sont inférieurs à ceux de CloudWatch. Pour plus d'informations, veuillez consulter Exportation de données de journal vers Amazon S3.

Bonnes pratiques relatives à Amazon EC2.

Vous pouvez utiliser les instances Amazon EC2 pour les flottes gérées par les services et les clients. Il y a trois considérations à prendre en compte :

- Pour les flottes gérées par des services, vous pouvez choisir d'avoir une ou plusieurs instances disponibles à tout moment en définissant le nombre minimum de travailleurs pour le parc. Lorsque vous définissez le nombre minimum de travailleurs au-dessus de 0, le parc compte toujours ce nombre de travailleurs actifs. Cela peut réduire le temps nécessaire à Deadline Cloud pour commencer à traiter les tâches, mais le temps d'inactivité de l'instance vous est facturé.
- Pour les flottes gérées par des services, définissez une taille maximale pour la flotte. Cela limite le nombre d'instances auxquelles une flotte peut s'adapter automatiquement. Les flottes ne dépasseront pas cette taille même si d'autres tâches attendent d'être traitées.
- Pour les flottes gérées par les services et celles gérées par le client, vous pouvez spécifier les types d'instances Amazon EC2 dans vos flottes. L'utilisation d'instances plus petites coûte moins cher par minute, mais peut prendre plus de temps pour terminer une tâche. À l'inverse, une instance plus grande coûte plus cher par minute, mais peut réduire le temps nécessaire à l'exécution d'une tâche. Comprendre les exigences que vos tâches imposent à une instance peut vous aider à réduire vos coûts.
- Dans la mesure du possible, choisissez des instances Amazon EC2 Spot pour votre flotte. Les instances ponctuelles sont disponibles à un prix réduit, mais peuvent être interrompues par des demandes à la demande. Les instances à la demande sont facturées à la seconde et ne sont pas interrompues.

Les meilleures pratiques pour AWS KMS

Par défaut, Deadline Cloud chiffre vos données à l'aide d'une clé que vous AWS possédez. Cette clé ne vous est pas facturée.

Vous pouvez choisir d'utiliser une clé gérée par le client pour chiffrer vos données. Lorsque vous utilisez votre propre clé, vous êtes facturé en fonction de la manière dont votre clé est utilisée. Si vous utilisez une clé existante, cela représentera un coût supplémentaire pour l'utilisation supplémentaire.

Les meilleures pratiques pour AWS PrivateLink

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion entre votre VPC et Deadline Cloud à l'aide d'un point de terminaison d'interface. Lorsque vous créez une connexion, vous pouvez

appeler toutes les actions de l'API Deadline Cloud. Vous êtes facturé par heure pour chaque point de terminaison que vous créez. Si vous l'utilisez PrivateLink, vous devez créer au moins trois points de terminaison, et selon votre configuration, vous en aurez peut-être besoin de cinq.

Bonnes pratiques pour Amazon S3

Deadline Cloud utilise Amazon S3 pour stocker les ressources à traiter, les pièces jointes aux tâches, les sorties et les journaux. Pour réduire les coûts associés à Amazon S3, réduisez la quantité de données que vous stockez. Quelques suggestions :

- Ne stockez que les actifs actuellement utilisés ou qui le seront prochainement.
- Utilisez une configuration S3 Lifecycle pour supprimer automatiquement les fichiers inutilisés d'un compartiment S3.

Bonnes pratiques pour Amazon VPC

Lorsque vous utilisez des licences basées sur l'utilisation pour votre flotte gérée par le client, vous créez un point de terminaison de licence Deadline Cloud, qui est un point de terminaison Amazon VPC créé dans votre compte. Ce terminal est facturé à un taux horaire. Pour réduire les coûts, supprimez les points de terminaison lorsque vous n'utilisez pas de licences basées sur l'utilisation.

Sécurité dans Deadline Cloud

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Deadline Cloud, voir Services AWS Portée par programme de conformitéServices AWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation Deadline Cloud. Les rubriques suivantes expliquent comment procéder à la configuration Deadline Cloud pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres outils Services AWS qui vous aident à surveiller et à sécuriser vos Deadline Cloud ressources.

Rubriques

- Bonnes pratiques de sécurité pour Deadline Cloud

Protection des données dans Deadline Cloud

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Deadline Cloud. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que

le champ Name (Nom). Cela inclut lorsque vous travaillez avec Deadline Cloud ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Rubriques

Chiffrement au repos

AWS Deadline Cloud protège les données sensibles en les chiffrant au repos à l'aide des clés de chiffrement stockées dans AWS Key Management Service (AWS KMS). Le chiffrement au repos est disponible partout Régions AWS où il Deadline Cloud est disponible.

Le chiffrement des données signifie que les données sensibles enregistrées sur les disques ne sont pas lisibles par un utilisateur ou une application sans clé valide. Seule une partie disposant d'une clé gérée valide peut déchiffrer les données.

Pour plus d'informations sur AWS KMS les Deadline Cloud utilisations du chiffrement des données au repos, consultezGestion des clés.

Chiffrement en transit

Pour les données en transit, AWS Deadline Cloud utilise le protocole TLS (Transport Layer Security) 1.2 ou 1.3 pour chiffrer les données envoyées entre le service et les employés. Nous exigeons TLS 1.2 et recommandons TLS 1.3. En outre, si vous utilisez un cloud privé virtuel (VPC), vous pouvez l'utiliser AWS PrivateLink pour établir une connexion privée entre votre VPC et. Deadline Cloud

Gestion des clés

Lorsque vous créez un nouveau parc de serveurs, vous pouvez choisir l'une des clés suivantes pour chiffrer les données de votre parc de serveurs :

- AWS clé KMS détenue : type de chiffrement par défaut si vous ne spécifiez pas de clé lors de la création du parc de serveurs. La clé KMS appartient à AWS Deadline Cloud. Vous ne pouvez pas afficher, gérer ou utiliser les clés que vous AWS possédez. Cependant, vous n'avez aucune action à effectuer pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section sur les clés AWS détenues dans le guide du AWS Key Management Service développeur.
- Clé KMS gérée par le client : vous spécifiez une clé gérée par le client lorsque vous créez un parc de serveurs. Tout le contenu de la ferme est chiffré à l'aide de la clé KMS. La clé est stockée dans votre compte et vous la créez, la détenez et la gérez. AWS KMS Des frais s'appliquent. Vous avez le contrôle total de la clé KMS. Vous pouvez effectuer des tâches telles que :
  - Établissement et mise à jour de politiques clés
  - Établissement et gestion des politiques IAM et des octrois
  - Activation et désactivation des stratégies de clé
  - Ajout de balises
  - Création d'alias de clé

  Vous ne pouvez pas faire pivoter manuellement une clé appartenant à un client utilisée avec une Deadline Cloud ferme. La rotation automatique de la clé est prise en charge.

  Pour plus d'informations, consultez la section Clés détenues par le client dans le Guide du AWS Key Management Service développeur.

  Pour créer une clé gérée par le client, suivez les étapes de création de clés gérées par le client symétriques dans le guide du AWS Key Management Service développeur.

Comment Deadline Cloud utiliser les AWS KMS subventions

Deadline Cloud nécessite une autorisation pour utiliser votre clé gérée par le client. Lorsque vous créez un parc chiffré à l'aide d'une clé gérée par le client, vous Deadline Cloud créez une autorisation en votre nom en envoyant une `CreateGrant` demande d'accès à la clé KMS que vous avez spécifiée. AWS KMS

Deadline Cloud utilise plusieurs subventions. Chaque autorisation est utilisée par un service différent Deadline Cloud qui doit chiffrer ou déchiffrer vos données. Deadline Cloud utilise également des subventions pour permettre l'accès à d'autres AWS services utilisés pour stocker des données en votre nom, tels qu'Amazon Simple Storage Service, Amazon Elastic Block Store ou OpenSearch.

Les subventions qui permettent Deadline Cloud de gérer les machines d'un parc géré par des services incluent un numéro de Deadline Cloud compte et un rôle au `GranteePrincipal` lieu d'un directeur de service. Bien que cela ne soit pas habituel, cela est nécessaire pour chiffrer les volumes Amazon EBS destinés aux employés des flottes gérées par des services à l'aide de la clé KMS gérée par le client spécifiée pour le parc de serveurs.

Politique de clé gérée par le client

Les politiques de clés contrôlent l'accès à votre clé gérée par le client. Chaque clé doit avoir exactement une politique clé contenant des instructions qui déterminent qui peut utiliser la clé et comment ils peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez définir une politique clé. Pour plus d'informations, consultez Gestion de l'accès aux clés gérées par le client dans le Guide du développeur AWS Key Management Service .

Politique IAM minimale pour CreateFarm

Pour utiliser votre clé gérée par le client afin de créer des fermes à l'aide de la console ou de l'opération d'`CreateFarm`API, les opérations d' AWS KMS API suivantes doivent être autorisées :

- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Accorde l'accès à la console à une AWS KMS clé spécifiée. Pour plus d'informations, consultez la section Utilisation des subventions dans le guide du AWS Key Management Service développeur.
- `kms:Decrypt`— Permet Deadline Cloud de déchiffrer les données de la ferme.
- `kms:DescribeKey`— Fournit les informations clés gérées par le client Deadline Cloud pour permettre de valider la clé.
- `kms:GenerateDataKey`— Permet de chiffrer Deadline Cloud les données à l'aide d'une clé de données unique.

La déclaration de politique suivante accorde les autorisations nécessaires à l'`CreateFarm`opération.

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

Politique IAM minimale pour les opérations en lecture seule

Utiliser votre clé gérée par le client pour des Deadline Cloud opérations en lecture seule, telles que l'obtention d'informations sur les fermes, les files d'attente et les flottes. Les opérations AWS KMS d'API suivantes doivent être autorisées :

- `kms:Decrypt`— Permet Deadline Cloud de déchiffrer les données de la ferme.
- `kms:DescribeKey`— Fournit les informations clés gérées par le client Deadline Cloud pour permettre de valider la clé.

La déclaration de politique suivante accorde les autorisations nécessaires pour les opérations en lecture seule.

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

Politique IAM minimale pour les opérations de lecture-écriture

Utiliser votre clé gérée par le client pour les Deadline Cloud opérations de lecture-écriture, telles que la création et la mise à jour de parcs, de files d'attente et de flottes. Les opérations AWS KMS d'API suivantes doivent être autorisées :

- `kms:Decrypt`— Permet Deadline Cloud de déchiffrer les données de la ferme.
- `kms:DescribeKey`— Fournit les informations clés gérées par le client Deadline Cloud pour permettre de valider la clé.
- `kms:GenerateDataKey`— Permet de chiffrer Deadline Cloud les données à l'aide d'une clé de données unique.

La déclaration de politique suivante accorde les autorisations nécessaires à l'`CreateFarm`opération.

```
{
    "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"
```

```
                }
            }
        }
    ]
}
```

Surveillance de vos clés de chiffrement

Lorsque vous utilisez une clé gérée par le AWS KMS client pour vos Deadline Cloud fermes, vous pouvez utiliser AWS CloudTrailAmazon CloudWatch Logs pour suivre les demandes Deadline Cloud envoyées à AWS KMS.

CloudTrail événement pour les subventions

L'exemple d' CloudTrail événement suivant se produit lorsque des autorisations sont créées, généralement lorsque vous appelez l'`CreateFleet`opération `CreateFarmCreateMonitor`, ou.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T02:05:26Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T02:05:35Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "operations": [
            "CreateGrant",
            "Decrypt",
            "DescribeKey",
            "Encrypt",
            "GenerateDataKey"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:deadline:farmId": "farm-abcdef1234567890098765432 1fedcba",
                "aws:deadline:accountId": "111122223333"
            }
        },
        "granteePrincipal": "deadline.amazonaws.com",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "retiringPrincipal": "deadline.amazonaws.com"
    },
    "responseElements": {
        "grantId": "6bbe819394822a400fe5e3a75d0e9ef16c1733143fff0c1fc00dc7ac282a18a0",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE44444"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
```

```
}
```

CloudTrail événement de déchiffrement

L'exemple d' CloudTrail événement suivant se produit lors du déchiffrement de valeurs à l'aide de la clé KMS gérée par le client.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:51:44Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
```

```
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "responseElements": null,
    "requestID": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeffffff",
    "eventID": "ffffffff-eeee-dddd-cccc-bbbbbbaaaaaa",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CloudTrail événement pour le chiffrement

L'exemple d' CloudTrail événement suivant se produit lors du chiffrement de valeurs à l'aide de la clé KMS gérée par le client.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
```

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

Supprimer une clé KMS gérée par le client

La suppression d'une clé KMS gérée par le client dans AWS Key Management Service (AWS KMS) est destructrice et potentiellement dangereuse. Il supprime de manière irréversible le contenu clé et toutes les métadonnées associées à la clé. Après la suppression d'une clé KMS gérée par le client, vous ne pouvez plus déchiffrer les données chiffrées par cette clé. Cela signifie que les données deviennent irrécupérables.

C'est pourquoi les AWS KMS clients disposent d'un délai d'attente pouvant aller jusqu'à 30 jours avant de supprimer la clé KMS. La période d'attente par défaut est de 30 jours.

À propos de la période d'attente

Comme il est destructeur et potentiellement dangereux de supprimer une clé KMS gérée par le client, nous vous demandons de définir un délai d'attente de 7 à 30 jours. La période d'attente par défaut est de 30 jours.

Cependant, la période d'attente réelle peut être supérieure de 24 heures à la période que vous avez planifiée. Pour obtenir la date et l'heure réelles auxquelles la clé sera supprimée, utilisez l'DescribeKeyopération. Vous pouvez également voir la date de suppression planifiée d'une clé dans la AWS KMS console sur la page détaillée de la clé, dans la section Configuration générale. Notez le fuseau horaire.

Pendant la période d'attente, le statut de la clé gérée par le client et l'état de la clé sont En attente de suppression.

- Une clé KMS gérée par le client en attente de suppression ne peut être utilisée dans aucune opération cryptographique.
- AWS KMS ne fait pas pivoter les clés de sauvegarde des clés KMS gérées par le client en attente de suppression.

Pour plus d'informations sur la suppression d'une clé KMS gérée par le client, consultez la section Suppression des clés principales du client dans le guide du AWS Key Management Service développeur.

Confidentialité du trafic inter-réseaux

AWS Deadline Cloud prend en charge Amazon Virtual Private Cloud (Amazon VPC) pour sécuriser les connexions. Amazon VPC fournit des fonctionnalités que vous pouvez utiliser pour renforcer et surveiller la sécurité de votre cloud privé virtuel (VPC).

Vous pouvez configurer un parc géré par le client (CMF) avec des instances Amazon Elastic Compute Cloud (Amazon EC2) exécutées au sein d'un VPC. En déployant les points de terminaison Amazon VPC à utiliser AWS PrivateLink, le trafic entre les travailleurs de votre CMF et le point de Deadline Cloud terminaison reste au sein de votre VPC. En outre, vous pouvez configurer votre VPC pour restreindre l'accès Internet à vos instances.

Dans les flottes gérées par des services, les employés ne sont pas joignables depuis Internet, mais ils ont accès à Internet et se connectent au Deadline Cloud service via Internet.

Se désinscrire

AWS Deadline Cloud collecte certaines informations opérationnelles pour nous aider à nous développer et à nous améliorer Deadline Cloud. Les données collectées incluent des éléments tels que votre identifiant de AWS compte et votre identifiant d'utilisateur, afin que nous puissions vous identifier correctement en cas de problème avec le Deadline Cloud. Nous collectons également Deadline Cloud des informations spécifiques, telles que les identifiants de ressource (un FarmID ou un QueueID le cas échéant), le nom du produit (par exemple, JobAttachments WorkerAgent, et plus encore) et la version du produit.

Vous pouvez choisir de ne pas participer à cette collecte de données en utilisant la configuration de l'application. Chaque ordinateur interagissant avec Deadline Cloud, à la fois les postes de travail des clients et les employés du parc, doit se désinscrire séparément.

Deadline Cloud moniteur - ordinateur de bureau

Deadline Cloud monitor - desktop collecte des informations opérationnelles, telles que les pannes et l'ouverture de l'application, pour nous aider à savoir quand vous rencontrez des problèmes avec l'application. Pour refuser la collecte de ces informations opérationnelles, rendez-vous sur la page des paramètres et désactivez Activer la collecte de données pour mesurer les performances de Deadline Cloud Monitor.

Une fois que vous vous êtes désinscrit, le moniteur de bureau n'envoie plus les données opérationnelles. Toutes les données précédemment collectées sont conservées et peuvent toujours être utilisées pour améliorer le service. Pour de plus amples informations, veuillez consulter FAQ sur la confidentialité des données.

AWS Deadline Cloud CLI et outils

La AWS Deadline Cloud CLI, les soumetteurs et l'agent de travail collectent tous des informations opérationnelles, telles que les cas de plantage et le moment où les tâches sont soumises, afin de

nous aider à savoir quand vous rencontrez des problèmes avec ces applications. Pour refuser la collecte de ces informations opérationnelles, utilisez l'une des méthodes suivantes :

- Dans le terminal, entrez**`deadline config set telemetry.opt_out true`**.

  Cela désactivera la CLI, les soumetteurs et l'agent de travail lors de l'exécution en tant qu'utilisateur actuel.
- Lors de l'installation de l' Deadline Cloud agent de travail, ajoutez l'argument de ligne de **`--telemetry-opt-out`** commande. Par exemple, **`./install.sh --farm-id $FARM_ID --fleet-id $FLEET_ID --telemetry-opt-out`**.
- Avant d'exécuter l'agent de travail, la CLI ou l'émetteur, définissez une variable d'environnement : **`DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true`**

Une fois que vous vous êtes désinscrit, les Deadline Cloud outils n'envoient plus les données opérationnelles. Toutes les données précédemment collectées sont conservées et peuvent toujours être utilisées pour améliorer le service. Pour de plus amples informations, veuillez consulter FAQ sur la confidentialité des données.

Identity and Access Management dans Deadline Cloud

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de Deadline Cloud. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Deadline Cloud.

Utilisateur du service : si vous utilisez le service Deadline Cloud pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Deadline Cloud pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Deadline Cloud, consultezRésolution des problèmes d'identité et d'accès à AWS Deadline Cloud.

Administrateur du service — Si vous êtes responsable des ressources de Deadline Cloud au sein de votre entreprise, vous avez probablement un accès complet à Deadline Cloud. C'est à vous de déterminer les fonctionnalités et les ressources de Deadline Cloud auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Deadline Cloud, consultezComment Deadline Cloud fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Deadline Cloud. Pour consulter des exemples de politiques basées sur l'identité de Deadline Cloud que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Deadline Cloud

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service.

FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des

documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour

contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS

Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Deadline Cloud fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Deadline Cloud, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Deadline Cloud.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Deadline Cloud

Fonction IAM	Support de Deadline Cloud
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui

Fonction IAM	Support de Deadline Cloud
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Deadline Cloud et les autres services Services AWS fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Deadline Cloud

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments

que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Deadline Cloud

Pour consulter des exemples de politiques basées sur l'identité de Deadline Cloud, consultez. Exemples de politiques basées sur l'identité pour Deadline Cloud

Politiques basées sur les ressources dans Deadline Cloud

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour Deadline Cloud

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de Deadline Cloud, consultez la section Actions définies par AWS Deadline Cloud dans la référence d'autorisation de service.

Les actions politiques dans Deadline Cloud utilisent le préfixe suivant avant l'action :

```
deadline
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "deadline:action1",
      "deadline:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité de Deadline Cloud, consultez. Exemples de politiques basées sur l'identité pour Deadline Cloud

Ressources relatives aux politiques pour Deadline Cloud

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Deadline Cloud et leurs ARN, consultez la section Ressources définies par AWS Deadline Cloud dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Deadline Cloud.

Pour consulter des exemples de politiques basées sur l'identité de Deadline Cloud, consultez. Exemples de politiques basées sur l'identité pour Deadline Cloud

Clés de conditions de politique pour Deadline Cloud

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition de Deadline Cloud, voir Clés de condition pour AWS Deadline Cloud dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Deadline Cloud.

Pour consulter des exemples de politiques basées sur l'identité de Deadline Cloud, consultez. Exemples de politiques basées sur l'identité pour Deadline Cloud

ACL dans Deadline Cloud

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Deadline Cloud

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Deadline Cloud

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous

créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour Deadline Cloud

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Deadline Cloud

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités de Deadline Cloud. Modifiez les rôles de service uniquement lorsque Deadline Cloud fournit des instructions à cet effet.

Rôles liés à un service pour Deadline Cloud

Prend en charge les rôles liés à un service	Non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Deadline Cloud

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Deadline Cloud. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Deadline Cloud, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour AWS Deadline Cloud dans la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Deadline Cloud dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Deadline Cloud

Pour accéder à la console AWS Deadline Cloud, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources de Deadline Cloud présentes dans votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Deadline Cloud, associez également le Deadline Cloud `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Politique de soumission des tâches à une file d'attente

Dans cet exemple, vous créez une politique limitée qui accorde l'autorisation de soumettre des tâches à une file d'attente spécifique dans un parc spécifique.

```
{
    "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/*"
        }
    ]
}
```

Politique autorisant la création d'un point de terminaison de licence

Dans cet exemple, vous créez une politique délimitée qui accorde les autorisations requises pour créer et gérer les points de terminaison de licence. Utilisez cette politique pour créer le point de terminaison de licence pour le VPC associé à votre parc de serveurs.

```
{
    "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": "*"
    }]
}
```

Politique autorisant la surveillance d'une file d'attente de ferme spécifique

Dans cet exemple, vous créez une politique limitée qui autorise le suivi des tâches dans une file d'attente spécifique pour un parc de serveurs spécifique.

```
{
    "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 politiques gérées pour Deadline Cloud

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSDeadlineCloud-FleetWorker

Vous pouvez associer la `AWSDeadlineCloud-FleetWorker` politique à vos identités AWS Identity and Access Management (IAM).

Cette politique accorde aux travailleurs de cette flotte les autorisations nécessaires pour se connecter au service et en recevoir des tâches.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `deadline`— Permet aux directeurs d'entreprise de gérer les travailleurs d'une flotte.

Pour obtenir une liste JSON des détails de la politique, voir AWSDeadlineCloud- FleetWorker dans le guide de référence des politiques gérées par AWS.

AWS politique gérée : AWSDeadlineCloud-WorkerHost

Vous pouvez associer la politique `AWSDeadlineCloud-WorkerHost` à vos identités IAM.

Cette politique accorde les autorisations nécessaires pour se connecter initialement au service. Il peut être utilisé comme profil d'instance Amazon Elastic Compute Cloud (Amazon EC2).

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `deadline`— Permet aux directeurs de créer des travailleurs.

Pour obtenir une liste JSON des détails de la politique, voir AWSDeadlineCloud- WorkerHost dans le guide de référence des politiques gérées par AWS.

AWS politique gérée : AWSDeadlineCloud-UserAccessFarms

Vous pouvez associer la politique `AWSDeadlineCloud-UserAccessFarms` à vos identités IAM.

Cette politique permet aux utilisateurs d'accéder aux données des fermes en fonction des fermes dont ils sont membres et de leur niveau d'adhésion.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `deadline`— Permet à l'utilisateur d'accéder aux données de la ferme.
- `ec2`— Permet aux utilisateurs de consulter les informations relatives aux types d'instances Amazon EC2.
- `identitystore`— Permet aux utilisateurs de voir les noms des utilisateurs et des groupes.

Pour obtenir une liste JSON des détails de la politique, consultez AWSDeadlineCloud- UserAccess Farms dans le guide de référence des politiques gérées par AWS.

AWS politique gérée : AWSDeadlineCloud-UserAccessFleets

Vous pouvez associer la politique `AWSDeadlineCloud-UserAccessFleets` à vos identités IAM.

Cette politique permet aux utilisateurs d'accéder aux données de la flotte en fonction des fermes dont ils sont membres et de leur niveau d'adhésion.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `deadline`— Permet à l'utilisateur d'accéder aux données de la ferme.
- `ec2`— Permet aux utilisateurs de consulter les informations relatives aux types d'instances Amazon EC2.
- `identitystore`— Permet aux utilisateurs de voir les noms des utilisateurs et des groupes.

Pour obtenir une liste JSON des détails de la politique, voir AWSDeadlineCloud « UserAccessFleets » dans le guide de référence des politiques gérées par AWS.

AWS politique gérée : AWSDeadlineCloud-UserAccessJobs

Vous pouvez associer la politique `AWSDeadlineCloud-UserAccessJobs` à vos identités IAM.

Cette politique permet aux utilisateurs d'accéder aux données relatives aux emplois en fonction des fermes dont ils sont membres et de leur niveau d'adhésion.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `deadline`— Permet à l'utilisateur d'accéder aux données de la ferme.
- `ec2`— Permet aux utilisateurs de consulter les informations relatives aux types d'instances Amazon EC2.
- `identitystore`— Permet aux utilisateurs de voir les noms des utilisateurs et des groupes.

Pour obtenir une liste JSON des détails de la politique, voir AWSDeadlineCloud « UserAccessJobs » dans le guide de référence des politiques gérées par AWS.

AWS politique gérée : AWSDeadlineCloud-UserAccessQueues

Vous pouvez associer la politique `AWSDeadlineCloud-UserAccessQueues` à vos identités IAM.

Cette politique permet aux utilisateurs d'accéder aux données des files d'attente en fonction des fermes dont ils sont membres et de leur niveau d'adhésion.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `deadline`— Permet à l'utilisateur d'accéder aux données de la ferme.
- `ec2`— Permet aux utilisateurs de consulter les informations relatives aux types d'instances Amazon EC2.
- `identitystore`— Permet aux utilisateurs de voir les noms des utilisateurs et des groupes.

Pour obtenir une liste JSON des détails de la politique, consultez AWSDeadlineCloud la section « AWSDeadlineCloud-UserAccessQueues » dans le guide de référence des politiques gérées par AWS.

Mises à jour des politiques AWS gérées par Deadline Cloud

Consultez les détails des mises à jour des politiques AWS gérées pour Deadline Cloud depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents de Deadline Cloud.

Modification	Description	Date
Deadline Cloud a commencé à suivre les modifications	Deadline Cloud a commencé à suivre les modifications apportées à ses politiques AWS gérées.	2 avril 2024

Résolution des problèmes d'identité et d'accès à AWS Deadline Cloud

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Deadline Cloud et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Deadline Cloud
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Deadline Cloud

Je ne suis pas autorisé à effectuer une action dans Deadline Cloud

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `deadline:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 deadline:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `deadline:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Deadline Cloud.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Deadline Cloud. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Deadline Cloud

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Deadline Cloud prend en charge ces fonctionnalités, consultezComment Deadline Cloud fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Validation de conformité pour Deadline Cloud

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider

à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Deadline Cloud

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

AWS Deadline Cloud ne sauvegarde pas les données stockées dans le compartiment S3 de vos pièces jointes aux tâches. Vous pouvez activer les sauvegardes des données de vos pièces jointes à des tâches à l'aide de n'importe quel mécanisme de sauvegarde standard d'Amazon S3, tel que le versionnement S3 ou AWS Backup.

Sécurité de l'infrastructure dans Deadline Cloud

En tant que service géré, AWS Deadline Cloud est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Deadline Cloud via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Deadline Cloud ne prend pas en charge l'utilisation de politiques de point de terminaison de cloud privé AWS PrivateLink virtuel (VPC). Il utilise la politique AWS PrivateLink par défaut, qui accorde un accès complet au point de terminaison. Pour plus d'informations, consultez la section Politique de point de terminaison par défaut dans le guide de AWS PrivateLink l'utilisateur.

Analyse de configuration et de vulnérabilité dans Deadline Cloud

AWS gère les tâches de sécurité de base telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre. Ces procédures ont été vérifiées et certifiées par les tiers appropriés. Pour plus de détails, consultez les ressources suivantes :

- Modèle de responsabilité partagée
- Amazon Web Services : Présentation des procédures de sécurité (livre blanc)

AWS Deadline Cloud gère les tâches sur les flottes gérées par les services ou par les clients :

- Pour les flottes gérées par des services, Deadline Cloud gère le système d'exploitation client.
- Pour les flottes gérées par le client, vous êtes responsable de la gestion du système d'exploitation.

Pour plus d'informations sur la configuration et l'analyse des vulnérabilités pour AWS Deadline Cloud, voir

- Bonnes pratiques de sécurité pour Deadline Cloud

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition aws:SourceAccountglobale aws:SourceArnet les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS Deadline Cloud accordent un autre service à la ressource. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger contre le problème de l'adjoint confus est d'utiliser la clé de `aws:SourceArn` contexte de condition globale avec le nom de ressource Amazon (ARN) complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:deadline:*:123456789012:*`.

Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.

L'exemple suivant montre comment vous pouvez utiliser les touches de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale Deadline Cloud pour éviter le problème de confusion des adjoints.

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

Accès AWS Deadline Cloud via un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et. AWS Deadline Cloud Vous pouvez y accéder Deadline Cloud comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour y accéder. Deadline Cloud

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à Deadline Cloud.

Pour plus d'informations, consultez Accès aux Services AWS via AWS PrivateLink dans le Guide AWS PrivateLink .

Considérations relatives à Deadline Cloud

Avant de configurer un point de terminaison d'interface pour Deadline Cloud, consultez la section Accès à un service AWS à l'aide d'un point de terminaison VPC d'interface dans le AWS PrivateLink Guide.

Deadline Cloud prend en charge les appels à toutes ses actions d'API via le point de terminaison de l'interface.

Par défaut, l'accès complet à Deadline Cloud est autorisé via le point de terminaison de l'interface. Vous pouvez également associer un groupe de sécurité aux interfaces réseau du point de terminaison pour contrôler le trafic Deadline Cloud passant par le point de terminaison de l'interface.

Deadline Cloud ne prend pas en charge les politiques de point de terminaison VPC. Pour plus d'informations, consultez la section Contrôler l'accès aux points de terminaison VPC à l'aide des politiques relatives aux points de terminaison dans le Guide.AWS PrivateLink

Deadline Cloud points de terminaison

Deadline Cloud utilise deux points de terminaison pour accéder au service en utilisant AWS PrivateLink.

Les travailleurs utilisent le `com.amazonaws.region.deadline.scheduling` point de terminaison pour récupérer les tâches de la file d'attente Deadline Cloud, rendre compte de la progression et renvoyer les résultats des tâches. Si vous utilisez une flotte gérée par le client, le point de terminaison de planification est le seul point de terminaison que vous devez créer, sauf si vous utilisez des opérations de gestion. Par exemple, si une tâche crée d'autres tâches, vous devez autoriser le point de terminaison de gestion à appeler l'`CreateJob`opération.

Le Deadline Cloud moniteur utilise le `com.amazonaws.region.deadline.management` pour gérer les ressources de votre ferme, par exemple en créant et en modifiant des files d'attente et des flottes ou en obtenant des listes de tâches, d'étapes et de tâches.

Deadline Cloud nécessite également des points de terminaison pour les points de terminaison AWS de service suivants :

- Deadline Cloud utilise AWS STS pour authentifier les travailleurs afin qu'ils puissent accéder aux actifs du travail. Pour plus d'informations AWS STS, consultez la section Informations d'identification de sécurité temporaires dans IAM dans le Guide de l'AWS Identity and Access Management utilisateur.
- Si vous configurez votre flotte gérée par le client dans un sous-réseau sans connexion Internet, vous devez créer un point de terminaison VPC pour CloudWatch Amazon Logs afin que les employés puissent écrire des journaux. Pour plus d'informations, consultez la section Surveillance avec CloudWatch.

- Si vous utilisez des pièces jointes à des tâches, vous devez créer un point de terminaison VPC pour Amazon Simple Storage Service (Amazon S3) afin que les employés puissent accéder aux pièces jointes. Pour plus d'informations, consultez la section Pièces jointes aux Job dans Deadline Cloud.

Créez des points de terminaison pour Deadline Cloud

Vous pouvez créer des points de terminaison d'interface pour Deadline Cloud utiliser la console Amazon VPC ou AWS Command Line Interface le AWS CLI(). Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez des points de terminaison de gestion et de planification pour Deadline Cloud utiliser les noms de service suivants. Remplacez *la région* par celle Région AWS où vous avez effectué le déploiement Deadline Cloud.

```
com.amazonaws.region.deadline.management
```

```
com.amazonaws.region.deadline.scheduling
```

Si vous activez le DNS privé pour les points de terminaison de l'interface, vous pouvez envoyer des demandes d'API à Deadline Cloud l'aide de son nom DNS régional par défaut. Par exemple, `worker.deadline.us-east-1.amazonaws.com` pour les opérations des travailleurs ou `management.deadline.us-east-1.amazonaws.com` pour toutes les autres opérations.

Vous devez également créer un point de terminaison pour AWS STS utiliser le nom de service suivant :

```
com.amazonaws.region.sts
```

Si votre flotte gérée par le client se trouve sur un sous-réseau sans connexion Internet, vous devez créer un point de terminaison CloudWatch Logs en utilisant le nom de service suivant :

```
com.amazonaws.region.logs
```

Si vous utilisez des pièces jointes pour transférer des fichiers, vous devez créer un point de terminaison Amazon S3 en utilisant le nom de service suivant :

```
com.amazonaws.region.s3
```

Bonnes pratiques de sécurité pour Deadline Cloud

AWS Deadline Cloud (Deadline Cloud) fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

> **Note**
>
> Pour plus d'informations sur l'importance de nombreux sujets liés à la sécurité, consultez le modèle de responsabilité partagée.

Protection des données

Pour des raisons de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer des comptes individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui vous aident à découvrir et à sécuriser les données personnelles stockées dans Amazon Simple Storage Service (Amazon S3).
- Si vous avez besoin de modules cryptographiques validés FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour de plus amples informations sur les points de terminaison FIPS disponibles, consultez Federal Information Processing Standard (FIPS) 140-2.

Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles, telles que les numéros de compte de vos clients, dans des champs de formulaire comme Name (Nom). Cela inclut lorsque vous travaillez avec AWS Deadline Cloud ou une autre solution Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez dans Deadline Cloud ou dans d'autres services peuvent être récupérées pour être incluses dans les journaux de diagnostic. Lorsque vous fournissez une URL à un serveur externe, n'incluez pas les informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

AWS Identity and Access Management autorisations

Gérez l'accès aux AWS ressources à l'aide des utilisateurs, des rôles AWS Identity and Access Management (IAM) et en accordant le moindre privilège aux utilisateurs. Établissez des politiques et des procédures de gestion des informations d'identification pour la création, la distribution, la rotation et la révocation des informations AWS d'accès. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Exécuter des tâches en tant qu'utilisateurs et en tant que groupes

Lorsque vous utilisez la fonctionnalité de file d'attente dans Deadline Cloud, il est recommandé de spécifier un utilisateur du système d'exploitation (OS) et son groupe principal afin que l'utilisateur du système d'exploitation dispose des autorisations les moins privilégiées pour les tâches de la file d'attente.

Lorsque vous spécifiez un « Exécuter en tant qu'utilisateur » (et un groupe), tous les processus relatifs aux tâches soumises à la file d'attente seront exécutés à l'aide de cet utilisateur du système d'exploitation et hériteront des autorisations de système d'exploitation associées à cet utilisateur.

Les configurations de flotte et de file d'attente se combinent pour établir une posture de sécurité. Du côté de la file d'attente, le rôle « Job exécuté en tant qu'utilisateur » et le rôle IAM peuvent être spécifiés pour utiliser le système d'exploitation et AWS les autorisations pour les tâches de la file d'attente. Le parc définit l'infrastructure (hôtes de travail, réseaux, stockage partagé monté) qui, lorsqu'elle est associée à une file d'attente particulière, exécute les tâches au sein de cette file. Les données disponibles sur les hôtes de travail doivent être accessibles par les jobs depuis une ou plusieurs files d'attente associées. La spécification d'un utilisateur ou d'un groupe permet de protéger les données des tâches contre les autres files d'attente, les autres logiciels installés ou les autres utilisateurs ayant accès aux hôtes de travail. Lorsqu'une file d'attente n'a pas d'utilisateur, elle s'exécute en tant qu'utilisateur agent qui peut se faire passer pour (`sudo`) n'importe quel utilisateur de

la file d'attente. Ainsi, une file d'attente sans utilisateur peut transférer des privilèges à une autre file d'attente.

Réseaux

Pour éviter que le trafic ne soit intercepté ou redirigé, il est essentiel de sécuriser comment et où le trafic de votre réseau est acheminé.

Nous vous recommandons de sécuriser votre environnement réseau de la manière suivante :

- Sécurisez les tables de routage du sous-réseau Amazon Virtual Private Cloud (Amazon VPC) pour contrôler le mode de routage du trafic de la couche IP.
- Si vous utilisez Amazon Route 53 (Route 53) comme fournisseur DNS dans la configuration de votre parc ou de votre station de travail, sécurisez l'accès à l'API Route 53.
- Si vous vous connectez à Deadline Cloud en dehors de celui-ci, par AWS exemple en utilisant des postes de travail sur site ou d'autres centres de données, sécurisez toute infrastructure réseau sur site. Cela inclut les serveurs DNS et les tables de routage sur les routeurs, les commutateurs et autres périphériques réseau.

Emplois et données sur les emplois

Les tâches Deadline Cloud s'exécutent dans le cadre de sessions sur des hôtes de travail. Chaque session exécute un ou plusieurs processus sur l'hôte de travail, qui nécessitent généralement que vous saisissiez des données pour produire une sortie.

Pour sécuriser ces données, vous pouvez configurer les utilisateurs du système d'exploitation avec des files d'attente. L'agent de travail utilise l'utilisateur du système d'exploitation de la file d'attente pour exécuter les sous-processus de session. Ces sous-processus héritent des autorisations de l'utilisateur du système d'exploitation de la file d'attente.

Nous vous recommandons de suivre les meilleures pratiques pour sécuriser l'accès aux données auxquelles ces sous-processus accèdent. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

Structure de la ferme

Vous pouvez organiser les flottes et les files d'attente de Deadline Cloud de nombreuses manières. Cependant, certains arrangements ont des implications en matière de sécurité.

Une ferme possède l'une des limites les plus sécurisées, car elle ne peut pas partager les ressources de Deadline Cloud avec d'autres fermes, notamment les flottes, les files d'attente et les profils de stockage. Cependant, vous pouvez partager AWS des ressources externes au sein d'un parc de serveurs, ce qui compromet les limites de sécurité.

Vous pouvez également établir des limites de sécurité entre les files d'attente d'une même batterie de serveurs en utilisant la configuration appropriée.

Suivez ces bonnes pratiques pour créer des files d'attente sécurisées dans le même parc de serveurs :

- Associez une flotte uniquement aux files d'attente situées dans la même limite de sécurité. Notez ce qui suit :
  - Une fois la tâche exécutée sur l'hôte de travail, les données peuvent rester, par exemple dans un répertoire temporaire ou dans le répertoire personnel de l'utilisateur de la file d'attente.
  - Le même utilisateur du système d'exploitation exécute toutes les tâches sur un hôte de flotte appartenant au service, quelle que soit la file d'attente à laquelle vous soumettez la tâche.
  - Une tâche peut laisser des processus s'exécuter sur un hôte de travail, ce qui permet aux tâches d'autres files d'attente d'observer d'autres processus en cours d'exécution.
- Assurez-vous que seules les files d'attente situées dans la même limite de sécurité partagent un compartiment Amazon S3 pour les pièces jointes aux tâches.
- Assurez-vous que seules les files d'attente situées dans les mêmes limites de sécurité partagent un même utilisateur du système d'exploitation.
- Sécurisez toutes les autres AWS ressources intégrées à la ferme jusqu'à la limite.

Files d'attente pour les offres d'emploi

Les pièces jointes aux tâches sont associées à une file d'attente qui utilise votre compartiment Amazon S3.

- Les pièces jointes aux tâches sont écrites et lues à partir d'un préfixe racine du compartiment Amazon S3. Vous spécifiez ce préfixe racine dans l'appel `CreateQueue` d'API.
- Le bucket a un correspondant`Queue Role`, qui spécifie le rôle qui accorde aux utilisateurs de la file d'attente l'accès au bucket et au préfixe racine. Lorsque vous créez une file d'attente, vous spécifiez l'`Queue Role`Amazon Resource Name (ARN) à côté du compartiment des pièces jointes aux tâches et du préfixe racine.

- Les appels autorisés aux opérations `AssumeQueueRoleForReadAssumeQueueRoleForUser`, et `AssumeQueueRoleForWorker` API renvoient un ensemble d'informations d'identification de sécurité temporaires pour le`Queue Role`.

Si vous créez une file d'attente et que vous réutilisez un compartiment Amazon S3 et un préfixe racine, des informations risquent d'être divulguées à des tiers non autorisés. Par exemple, QueueA et QueueB partagent le même bucket et le même préfixe racine. Dans un flux de travail sécurisé, ArtistA a accès à QueueA mais pas à QueueB. Toutefois, lorsque plusieurs files d'attente partagent un bucket, ArtistA peut accéder aux données contenues dans QueueB car il utilise le même bucket et le même préfixe racine que QueueA.

La console configure des files d'attente sécurisées par défaut. Assurez-vous que les files d'attente comportent une combinaison distincte de compartiment Amazon S3 et de préfixe racine, sauf si elles font partie d'une limite de sécurité commune.

Pour isoler vos files d'attente, vous devez configurer le `Queue Role` pour autoriser uniquement l'accès aux files d'attente au bucket et au préfixe racine. Dans l'exemple suivant, remplacez chaque *`espace réservé par les informations`* spécifiques à votre ressource.

```
{
  "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/*"
    }
  ]
}
```

Vous devez également définir une politique de confiance pour le rôle. Dans l'exemple suivant, remplacez le texte de l'*espace réservé* par les informations spécifiques à votre ressource.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    },
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "credentials.deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    }
  ]
}
```

Buckets Amazon S3 logiciels personnalisés

Vous pouvez ajouter l'instruction suivante à votre compte `Queue Role` pour accéder aux logiciels personnalisés de votre compartiment Amazon S3. Dans l'exemple suivant, remplacez *SOFTWARE_BUCKET_NAME par le nom* de votre compartiment S3.

```
"Statement": [
    {
        "Action": [
            "s3:GetObject",
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME",
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME/*"
        ]
    }
]
```

Pour plus d'informations sur les meilleures pratiques de sécurité d'Amazon S3, consultez la section Meilleures pratiques de sécurité pour Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Hôtes de travail

Sécurisez les hôtes de travail pour garantir que chaque utilisateur ne peut effectuer des opérations que pour le rôle qui lui est assigné.

Nous recommandons les meilleures pratiques suivantes pour sécuriser les hôtes de travail :

- N'utilisez pas la même `jobRunAsUser` valeur avec plusieurs files d'attente, sauf si les tâches soumises à ces files d'attente se situent dans la même limite de sécurité.
- Ne définissez pas la file `jobRunAsUser` d'attente sur le nom de l'utilisateur du système d'exploitation sous lequel l'agent de travail s'exécute.
- Accordez aux utilisateurs de la file d'attente les autorisations de système d'exploitation les moins privilégiées requises pour les charges de travail de file d'attente prévues. Assurez-vous qu'ils ne disposent pas d'autorisations d'écriture dans le système de fichiers pour accéder aux fichiers du programme de l'agent de travail ou à d'autres logiciels partagés.
- Assurez-vous que seuls l'utilisateur root Linux et le compte `Administrator` propriétaire sont propriétaires et peuvent modifier les fichiers du programme de l'agent de travail. Windows
- Sur les hôtes de Linux travail, envisagez de configurer une `umask` dérogation permettant à `/etc/sudoers` l'utilisateur de l'agent de travail de lancer des processus en tant qu'utilisateurs de la file d'attente. Cette configuration permet de garantir que les autres utilisateurs ne peuvent pas accéder aux fichiers écrits dans la file d'attente.

- Accordez à des personnes de confiance un accès moins privilégié aux hôtes professionnels.
- Limitez les autorisations permettant de remplacer les fichiers de configuration du DNS local (activé `/etc/hosts` et activé) Linux et `C:\Windows\system32\etc\hosts` de Windows router les tables sur les postes de travail et les systèmes d'exploitation des hôtes de travail.
- Limitez les autorisations relatives à la configuration DNS sur les postes de travail et les systèmes d'exploitation hôtes des travailleurs.
- Appliquez régulièrement des correctifs au système d'exploitation et à tous les logiciels installés. Cette approche inclut les logiciels spécifiquement utilisés avec Deadline Cloud, tels que les émetteurs, les adaptateurs, les agents de travail, les OpenJD packages, etc.
- Utilisez des mots de passe forts pour la Windows file d'attente`jobRunAsUser`.
- Changez régulièrement les mots de passe de votre file d'attente`jobRunAsUser`.
- Garantissez l'accès aux secrets des mots de Windows passe avec le moindre privilège et supprimez les secrets non utilisés.
- N'`jobRunAsUser`autorisez pas la file d'attente à exécuter les commandes de planification à l'avenir :
  - ActivéLinux, refusez à ces comptes l'accès à `cron` et`at`.
  - ActivéWindows, refusez à ces comptes l'accès au Windows planificateur de tâches.

> **Note**
>
> Pour plus d'informations sur l'importance d'appliquer régulièrement des correctifs au système d'exploitation et aux logiciels installés, consultez le modèle de responsabilité partagée.

Stations de travail

Il est important de sécuriser les postes de travail ayant accès à Deadline Cloud. Cette approche permet de garantir que les tâches que vous soumettez à Deadline Cloud ne peuvent pas exécuter des charges de travail arbitraires facturées à votre compte. Compte AWS

Nous recommandons de suivre les bonnes pratiques suivantes pour sécuriser les postes de travail des artistes. Pour plus d'informations, consultez le Modèle de responsabilité partagée .

- Sécurisez toutes les informations d'identification persistantes donnant accès à Deadline Cloud AWS, y compris. Pour de plus amples informations, veuillez consulter Gestion des clés d’accès pour les utilisateurs IAM dans le Guide de l’utilisateur IAM.
- Installez uniquement des logiciels fiables et sécurisés.
- Exigez que les utilisateurs se fédérent avec un fournisseur d'identité pour accéder à l' AWS aide d'informations d'identification temporaires.
- Utilisez des autorisations sécurisées sur les fichiers du programme d'envoi de Deadline Cloud pour éviter toute falsification.
- Accordez aux personnes de confiance un accès moins privilégié aux postes de travail des artistes.
- Utilisez uniquement les émetteurs et les adaptateurs que vous obtenez via le Deadline Cloud Monitor.
- Limitez les autorisations `/etc/hosts` et routez les tables sur les postes de travail et les systèmes d'exploitation hôtes des travailleurs.
- Limitez les autorisations `/etc/resolv.conf` aux postes de travail et aux systèmes d'exploitation hôtes des travailleurs.
- Appliquez régulièrement des correctifs au système d'exploitation et à tous les logiciels installés. Cette approche inclut les logiciels spécifiquement utilisés avec Deadline Cloud, tels que les émetteurs, les adaptateurs, les agents de travail, les OpenJD packages, etc.

Surveillance de AWS Deadline Cloud

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de AWS Deadline Cloud (Deadline Cloud) et de vos AWS solutions. Collectez des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Avant de commencer à surveiller Deadline Cloud, vous devez créer un plan de surveillance comprenant des réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- A quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

AWS et Deadline Cloud fournissent des outils que vous pouvez utiliser pour surveiller vos ressources et répondre aux incidents potentiels. Certains de ces outils assurent la surveillance à votre place, d'autres nécessitent une intervention manuelle. Vous devez automatiser les tâches de surveillance autant que possible.

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

  Deadline Cloud dispose de trois CloudWatch indicateurs.

- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux

dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.

- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Enregistrement des appels avec CloudTrail

AWS Deadline Cloud est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS dans Deadline Cloud. CloudTrail capture tous les appels d'API pour Deadline Cloud sous forme d'événements. Les appels capturés incluent des appels provenant de la console Deadline Cloud et des appels de code vers les opérations de l'API Deadline Cloud.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Deadline Cloud. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Deadline Cloud, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur le Deadline Cloud dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Deadline Cloud, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

CloudTrail enregistre également les événements lorsque les utilisateurs se connectent au moniteur Deadline Cloud et reçoivent des AWS informations d'identification. Lorsqu'un utilisateur se connecte, un CloudTrail événement se produit avec la source `signin.amazonaws.com` et le nom`UserAuthentication`. Un deuxième événement se produit lorsque l'utilisateur connecté reçoit des informations d' AWS identification provenant de la source `sts.amazonaws.com` et du nom. `AssumeRole` L'identifiant de l'utilisateur est enregistré dans le deuxième événement dans le nom de session du rôle.

Pour un enregistrement continu des événements de votre site Compte AWS, y compris des événements pour Deadline Cloud, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence.

Pour plus d'informations, consultez les ressources suivantes :

Présentation de la création d'un journal de suivi

CloudTrail services et intégrations pris en charge

Configuration des notifications Amazon SNS pour CloudTrail

Réception de fichiers CloudTrail journaux provenant de plusieurs régions

Réception de fichiers CloudTrail journaux provenant de plusieurs comptes

Deadline Cloud prend en charge l'enregistrement des actions suivantes sous forme d'événements dans des fichiers CloudTrail journaux :

- associate-member-to-farm
- associate-member-to-fleet
- associate-member-to-job
- associate-member-to-queue
- assume-fleet-role-for-lire
- assume-fleet-role-for-travailleur
- assume-queue-role-for-lire
- assume-queue-role-for-utilisateur
- assume-queue-role-for-travailleur
- créer un budget
- créer une ferme
- create-fleet
- create-license-endpoint
- créer un moniteur
- créer une file
- create-queue-environment
- create-queue-fleet-association
- create-storage-profile
- create-worker
- supprimer-budget
- supprime-ferme
- delete-fleet
- delete-license-endpoint
- delete-metered-product
- supprimer-moniteur
- supprimer-file
- delete-queue-environment
- delete-queue-fleet-association
- delete-storage-profile

- supprime-travailleur
- disassociate-member-from-farm
- disassociate-member-from-fleet
- disassociate-member-from-job
- disassociate-member-from-queue
- get-application-version
- obtenir un budget
- get-farm
- get-feature-map
- get-fleet
- get-license-endpoint
- get-monitor
- get-queue
- get-queue-environment
- get-queue-fleet-association
- get-sessions-statistics-aggregation
- get-storage-profile
- get-storage-profile-for-file d'attente
- list-available-metered-products
- liste-budgets
- list-farm-members
- listez les fermes
- list-fleet-members
- listes de flottes
- list-job-members
- list-license-endpoints
- list-metered-products
- moniteurs de liste

- list-queue-environments
- list-queue-fleet-associations
- list-queue-members
- files d'attente
- list-storage-profiles
- list-storage-profiles-for-file d'attente
- list-tags-for-resource
- put-metered-product
- start-sessions-statistics-aggregation
- tag-resource
- untag-resource
- mise à jour du budget
- ferme de mise à jour
- mettre à jour le parc
- moniteur de mise à jour
- file d'attente de mise à jour
- update-queue-environment
- update-queue-fleet-association
- update-storage-profile
- agent de mise à jour

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été effectuée par un autre service .

Pour plus d'informations, consultez l'élément Identité de l'CloudTrailutilisateur.

Comprendre les entrées du fichier journal de Deadline Cloud

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Cet exemple JSON montre le journal généré par un appel à l'**`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",
}
```


L'exemple montre la AWS région, l'adresse IP et d'autres « `requestParameters` » tels que le « `displayName` » et le « `kmsKeyArn` » qui peuvent vous aider à identifier l'événement.

Surveillance avec CloudWatch

Amazon CloudWatch (CloudWatch) collecte des données brutes et les transforme en indicateurs lisibles en temps quasi réel. Vous pouvez ouvrir la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/ pour consulter et filtrer les métriques de Deadline Cloud.

- Dans un parc géré par le client de Deadline Cloud, vous CloudWatch envoie deux statistiques `UnhealthyWorkerCount` et : `RecommendedFleetSize`
- L'espace de noms pour ces métriques est `AWS/DeadlineCloud.`
- Vous pouvez utiliser les dimensions `farmID` et `fleetID` filtrer les métriques.
- Les deux métriques utilisent l'unité`count`.

Ces statistiques sont conservées pendant 15 mois afin que vous puissiez accéder aux informations historiques afin d'avoir une meilleure idée des performances de votre application ou service

Web. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Deadline Cloud possède deux types de journaux : les journaux des tâches et les journaux des travailleurs. Un journal des tâches se produit lorsque vous exécutez des journaux d'exécution sous forme de script ou lors de l'exécution de DCC. Un journal des tâches peut afficher des événements tels que le chargement de ressources, le rendu des tuiles ou l'impossibilité de trouver des textures.

Un journal des travailleurs indique les processus des agents des travailleurs. Cela peut inclure des éléments tels que le moment où les agents de travail démarrent, s'enregistrent, signalent les progrès, chargent des configurations ou terminent des tâches.

Pour Deadline Cloud, les employés téléchargent ces CloudWatch journaux dans Logs. Par défaut, les journaux n'expirent jamais. Si une tâche produit un volume élevé de données, vous pouvez encourir des coûts supplémentaires. Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

Vous pouvez ajuster la politique de rétention pour chaque groupe de journaux. Une durée de conservation plus courte permet de supprimer les anciens journaux et de réduire les coûts de stockage. Pour conserver les journaux, vous pouvez les archiver sur Amazon Simple Storage Service avant de les supprimer. Pour plus d'informations, consultez Exporter les données du journal vers Amazon S3 à l'aide de la console dans le guide de CloudWatch l'utilisateur Amazon.

> **Note**
>
> CloudWatch les lectures du journal sont limitées par AWS. Si vous prévoyez d'intégrer de nombreux artistes, nous vous suggérons de contacter AWS le service client et de demander une augmentation du `GetLogEvents` quota en CloudWatch. En outre, nous vous recommandons de fermer le portail de suivi des journaux lorsque vous n'êtes pas en train de déboguer.

Pour plus d'informations, consultez la section Quotas de CloudWatch journaux dans le guide de CloudWatch l'utilisateur Amazon.

Agir en fonction EventBridge des événements

Deadline Cloud envoie des événements EventBridge à Amazon pour vous informer des modifications apportées à l'état du service. Vous pouvez utiliser EventBridge ces événements pour rédiger des

règles qui prennent des mesures, par exemple pour vous avertir en cas de modification de votre flotte. Pour plus d'informations, consultez Qu'est-ce qu'Amazon ? EventBridge

Modification des recommandations relatives à la taille du parc

Lorsque vous configurez votre flotte pour utiliser le dimensionnement automatique basé sur les événements, Deadline Cloud envoie des événements que vous pouvez utiliser pour gérer vos flottes. Chacun de ces événements contient des informations sur la taille actuelle et la taille demandée d'une flotte. Pour un exemple d'utilisation d'un EventBridge événement et un exemple de fonction Lambda pour gérer l'événement, consultez. Faites évoluer automatiquement votre flotte Amazon EC2 grâce à la fonction de recommandation de dimensionnement de Deadline Cloud

L'événement de modification de la recommandation de taille de flotte est envoyé lorsque les événements suivants se produisent :

- Lorsque la taille de flotte recommandée change et `oldFleetSize` est différente de`newFleetSize`.
- Lorsque le service détecte que la taille réelle de la flotte ne correspond pas à la taille de flotte recommandée. Vous pouvez obtenir la taille réelle de la flotte à partir de la `workerCount` réponse de l'GetFleetopération. Cela peut se produire lorsqu'une instance Amazon EC2 active ne parvient pas à s'enregistrer en tant que travailleur de Deadline Cloud.

Le format de l'événement est le suivant :

```
{
    "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,
    }
}
```

Les champs suivants définissent le modèle d'événement :

`"source": "aws.deadline"`

Identifie que la source de cet événement est Deadline Cloud.

`"detail-type": "Fleet Size Recommendation Change"`

Identifie le type d'événement.

`"detail": { }`

Fournit des informations sur les modifications recommandées de la taille du parc.

`"farmId": "farm-12345678900000000000000000000000"`

Identifiant de la ferme qui contient la flotte.

`"fleetId": "fleet-12345678900000000000000000000000"`

Identifiant de la flotte dont la taille doit être modifiée.

`"oldFleetSize": 1`

La taille actuelle de la flotte.

`"newFleetSize": 5`

La nouvelle taille recommandée de la flotte.

Quotas pour Deadline Cloud

AWS Deadline Cloud fournit des ressources, telles que des fermes, des flottes et des files d'attente, que vous pouvez utiliser pour traiter les tâches. Lorsque vous créez votre Compte AWS, nous définissons des quotas par défaut pour chacune de ces ressources Région AWS.

Service Quotas est un emplacement central où vous pouvez consulter et gérer vos quotas pour Services AWS. Vous pouvez également demander une augmentation du quota pour la plupart des ressources que vous utilisez.

Pour consulter les quotas pour Deadline Cloud, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez Services AWSet sélectionnez Deadline Cloud.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le formulaire d'augmentation des quotas de service.

Création de ressources AWS Deadline Cloud avec AWS CloudFormation

AWS Deadline Cloud est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (telles que les fermes, les files d'attente et les flottes), puis vous AWS CloudFormation approvisionnez et configurez ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Deadline Cloud de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources encore et encore dans plusieurs Comptes AWS régions.

Deadline Cloud et AWS CloudFormation modèles

Pour fournir et configurer des ressources pour Deadline Cloud et les services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l'utilisateur.

Deadline Cloud prend en charge la création de fermes, de files d'attente et de flottes. AWS CloudFormationPour plus d'informations, notamment des exemples de modèles JSON et YAML pour les fermes, les files d'attente et les flottes, consultez le AWS Deadline Cloud dans le guide de l'AWS CloudFormation utilisateur.

En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation API Reference
- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

Historique des documents pour le guide de l'utilisateur de Deadline Cloud

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de l'utilisateur de AWS Deadline Cloud.

Modification	Description	Date
Première version	Il s'agit de la version initiale du guide de l'utilisateur de Deadline Cloud.	2 avril 2024

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.